HP LaserJet Security Drawer Statement

Hard Disk Data Security for HP LaserJet Printing Devices

Hard Disk Data Security for HP LaserJet Printing Devices

Introduction
Digital copier hard drives have been reported to retain "*an image of every document copied, scanned, or emailed by the machine*", which can be later retrieved.

HP LaserJet Multifunction printers and some models of HP LaserJet printers contain a hard disk drive (HDD). The following topics describe how data is managed on printing device HDDs.

Document Image Interaction with the Hard Disk
The HP printing device hard disk is involved in document processing in the following ways:

- Standard print and copy jobs print directly without storing information on the HDD. Advanced output options can use the HDD for temporary files.

- E-mail, Fax and Network folder scan jobs use the HDD for temporary files. These files are deleted as part of processing the job and are never retained permanently on the HDD.

- There is no feature or setting to retain standard print and scan jobs permanently on the HDD, with the exception of Stored Faxes, which temporarily store incoming faxes until released with a Fax PIN.

User Initiated Stored Documents
Documents can be stored on the device hard disk intentionally by customers when using the "Stored Jobs" feature. The system can be configured to automatically delete these jobs at 1 hour, 4 hour, 1 day, or 1 week intervals.

These jobs include

- Stored Jobs
- Personal Jobs
- Quick Copy Jobs
- Proof & Hold Jobs

HP Secure Data Erase Technology
The Secure File Erase feature ensures any hard disk information from print, copy, fax, and scan jobs is securely removed. This capability is provided as a standard feature on HP LaserJet MFPs and printers.

When this data is deleted, the hard disk areas containing the information are filled with random data using either a 1 pass or 3 pass overwrite, ensuring that the information cannot be recovered using diagnostic tools.

This overwrite technology is compliant with the US Government standard defined in NIST SP 800-88.

Protecting Data at Rest
When customer information is present on the hard disk, either as temporary job files or user created Stored Jobs, this is referred to as "Data at rest". This data can be protected using encryption or authentication such as a job PIN.

The HP Secure Hard Disk solution protects "data at rest" using encryption. All data written to the HP Secure Hard Disk is encrypted using the AES 128 encryption standard. If the hard disk is removed from the system, the encrypted information on the disk is not readable.

Stored and Personal jobs can be configured with a PIN by the user to protect others from printing them at the printing device control panel.

Customer Available Disk Sanitization Features
All information on an HP printing device hard disk can be securely deleted by the customer before disposal, redeployment or end of lease return.

The HP Secure Storage Erase feature overwrites the entire hard disk using HP Secure Data Erase technology (detailed above) with either a 1 pass or 3 pass overwrite. Performing Secure Storage Erase ensures all customer data is securely erased.

When using the HP Secure Hard Disk solution, all data present on the disk can be deleted by using "Secure Hard Disk Erase/Unlock", which performs a cryptographic erase. This feature of encrypted storage devices renders all data permanently unreadable by resetting the internal encryption keys.

For failed hard disk devices, HP offers a "Defective Media Retention" Carepack. This service allows customers to maintain possession of failed disk storage devices while adjuring to terms and conditions of standard warranty agreements. See www.hp.com/go/carepack for more information.

Customer Data Sanitization by HP
HP understands customer hard disks may contain sensitive business or technological information and employs appropriate security measures using standard industrial practices to safeguard that information.

For hard disks returned to HP refurbish or recycle facilities, the follow procedures are followed.

- Functional hard disks are wiped with a destructive data pattern to all addressable locations.
- Non-functional drives are recycled by crushing at a metal separation plant.

Note: Customers with regulatory or government requirements for data confidentiality are encouraged to maintain custody of the storage device or execute the onboard printing device's data sanitization procedures before releasing the device.

Summary

HP is committed to continually monitoring security issues to insure that our products are as secure as possible. We recommend that you visit hp.com for your particular printer model and visit our secure printing website (www.hp.com/go/secureprinting) for other important security information.