**Hard Disk Security**
Printers, multifunction printers, and copiers

# Hard Disk Security for Printers, MFPs, and Copiers

## What you need to know to protect your confidential information

# Hard disk security
## Risks, safeguards, and solutions

**It's common knowledge that computers store information on hard disk drives.** What's not as well known is that some printers and most multifunction printers (MFPs) and copiers also contain hard disk drives that record and store data. Residual data that may remain on the disk after printing, copying, etc. could pose a security risk.

### Your confidential data at risk

Recent reports on the *CBS Evening News* and *60 Minutes* demonstrated the security risks to data stored on MFP hard disk drives. In these reports CBS recovered dozens of pages of confidential information stored on MFPs, warehoused in several used equipment facilities.

The purpose of this document is to help Xerox customers become more secure in their knowledge of hard disk security issues and solutions. Understanding the potential risks and safeguards—and the advantages Xerox products provide—will help you prevent the loss of valuable intellectual assets and confidential data.

### Printer, MFP and copier hard disks

Digital information is transmitted to a printing device by a computer over a network, by scanning, or through a telephone line. Often this data is stored on a hard disk drive. This storage capacity enables the device to print faster and multitask—perform more than one function (print/copy/scan) simultaneously.

### How to tell if your printer or MFP has a hard disk drive

A comprehensive list of Xerox products and their standard or optional hard disks and security features is available at **www.xerox.com/security**. Click on the *Data Protection: Image Overwrite, Encryption and Disk Removal* link to download the PDF.

If the hard disk for your product is optional, there are two simple methods to determine if your specific model has a hard disk drive. From the control panel of your printer or MFP, locate and print the page that lists its configuration information. On the page, locate the entry for *Hard Disk*—or *Image Disk*, as it's sometimes referred to.

An alternative if your device is networked, is to connect to its built-in web server by entering its network IP address into the web browser on your PC. Once connected, click on the *Properties* link or tab and review the hardware specs. Look for information on its *Hard Disk* or *Image Disk*.

## How to protect your data

With the introduction of the first Xerox digital products, we recognized the potential security risks to stored data. The robust safeguards built into our products early on, like Disk Image Overwrite and Data Encryption, ensure data security from installation and setup, through the productive life of the product, to its eventual recycling or disposition.

## Disk Image Overwrite

The Disk Image Overwrite feature "scrubs" the disk drive in accordance with stringent specifications established by the US Department of Defense (DoD). This option became a standard feature on nearly every product in the Office portfolio in 2006.

The Disk Image Overwrite feature can be customized to remove all data from the hard disk according to your security needs:

- **Immediate**—automatic data overwrite immediately after printing is complete.
- **Scheduled**—automatic, daily data overwrite.
- **On Demand**—overwrite as needed, prior to disk removal, or at end-of-life device disposition.

## Hard Disk Removal Program

Xerox also established a disk drive removal program for all Xerox products. This program provide secure removal of the device's hard disk, so that it remains in your possession even if the printing device is traded in, recycled, or disposed. This program provides an alternative solution for the minority of products without the Disk Image Overwrite feature. Contact Xerox Customer Support for more information on fees and availability for your location.

## Data encryption

Most Xerox products equipped with hard disks also include our data encryption feature. When enabled, it encrypts all stored data with a state-of-the-art Advanced Encryption Standard (AES) 128-bit encryption algorithm.

## Safeguards for disposition

When a printer, MFP, or copier reaches the end of its useful life, it's ready to trade-in, recycle, donate, or dispose. But how can you be assured any residual intellectual or confidential property on the hard drive isn't at risk? Here's a simple process to follow for Xerox products, to protect your data:

1. Determine whether the printer, MFP, or copier being retired is equipped with a hard disk.
2. If the Xerox product is equipped with a hard disk, enable the Disk Image Overwrite function and "scrub" the disk.
3. If the product doesn't include the Disk Image Overwrite function, you may be able to use a third party software to overwrite the disk. You can also arrange removal of the hard disk by Xerox, your reseller, or remove it yourself.
4. Xerox provides several venues for the disposition of used equipment including our Trade-In Program, product recycling, and donation referrals for equipment with some remaining usable life. It is in your best interest to ensure you have overwritten or removed the hard disk prior to the product leaving your facility. While Xerox will make every reasonable effort to safeguard any residual data that remains on a product provided for trade-in or recycling, we can not guarantee its safety. The best practice is for the device owner to remove any confidential data prior to disposition.

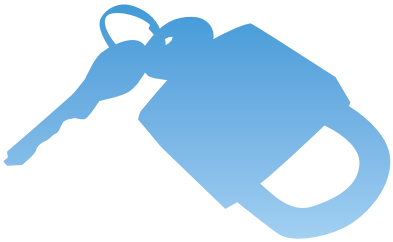
For more information on product disposition see **www.xerox.com/security**

## Security safeguards to look for when buying a new printer or MFP

- ☐ Hard disk drive image overwrite with a DoD-approved three-pass algorithm
- ☐ Hard disk drive data encryption with an AES encryption algorithm
- ☐ Hard disk removal option
- ☐ Network security support for SSL, IPsec, and SNMPv3
- ☐ Device authentication to control, manage, and track device access
- ☐ Secure fax
- ☐ Secure print feature
- ☐ Customer security alert process
- ☐ Secure product disposition process

## Product/feature availability

A comprehensive list of Xerox products with hard disks and their available security features is provided in the *Data Protection: Image Overwrite, Encryption and Disk Removal* document. Download the PDF at **www.xerox.com/security**



# Hard disk security
## Additional Xerox product security features

### Beyond hard disk security

In addition to data storage protection, Xerox products provide robust safeguards for data as it's being used.

### Network security

Xerox products are compatible with multiple network security protocols. The Secure Sockets Layer (SSL) protocol is used for secure job communication and reporting. The IPsec protocol protects network channels for DNS, DHCP, IPP, lpr, and Port 9100 printing. SNMPv3 is used for encrypted device management.

### Securing device use

**Firewall**—a built-in firewall manages all communication access to prevent unauthorized use.

**Authentication**—network authentication validates user names and/or passwords prior to device use. It can also be configured to allow or deny access to specific device functions such as scan, email, or fax functions. For additional security, the device may be configured to require log in by IT staff in order to change access or other configuration settings.

**Internal audit log**—Xerox MFPs and many of our printers can maintain audit logs to track activity by document, user, and function.

**Ports and services**—Unused ports and services can be shut off to prevent unauthorized access or malicious use.

**Embedded fax**—Unprotected fax connections in MFPs can be a back door into the network. Xerox was the first manufacturer to offer Common Criteria-certified products with fax communications internally separated from other network functions.

**Securing the output tray**—On a shared device in an office environment the output tray of a printer or MFP can be a security risk. Our Secure Print feature enables a user to send a job to print, where it will wait in the queue, until they enter a password (PIN) on the device's control panel to release the job. This feature is ideal for printing confidential documents securely on a workgroup device.

**Robust security made easy**—It's one thing to provide stringent security features and safeguards for MFPs and printers. But if they aren't easy to set-up and use, your company data may continue to be at risk. Xerox makes system administration and device management easy. Our free software, CentreWare® Web, allows IT staff access to device configuration, control, and management over the network through an easy-to-use browser-based interface.

### Additional data vulnerability

With all of the attention on security of digital information security, another critical point of potential security leaks may go unnoticed: paper documents. Paper documents are generally unsecured or locked in file cabinets. Often years worth of proprietary or confidential data is kept on file under minimal security in rows of file cabinets.

Xerox offers powerful scanning solutions that can automate the conversion of paper documents into secure, searchable digital archives. Storing your proprietary records digitally is not only more secure than paper documents, it's also more efficient and less expensive. Xerox scanning solutions provide an impressive ROI. They often pay for themselves in as little as six months.

For more information on our Scan to PC Desktop®, ScanFlowStore®, and DocuShare® Express solutions visit **www.xerox.com/office/software-solutions**

#### Security vigilance and alerts

Xerox is the only printer manufacturer with an active security patch program. We consistently monitor for new vulnerabilities on our MFPs, just as operating system software developers track new viruses that could threaten their software. Xerox security bulletins are posted on **www.xerox.com/security.** Customers can sign up for the RSS feed to be alerted immediately when a new bulletin or downloadable patch is posted.

For more information on Xerox security or to subscribe to our security RSS feed visit **www.xerox.com/security**