



Xerox Corporation

Copier/MFP Security Fact Sheet

Updated: June 4, 2010

General

- Xerox works directly with its customers to assess their security needs: identify where their information resides, how it is transferred and detect the greatest areas of risk.
- Xerox estimates that large enterprises create more than 850 million impressions of their data per year using printers and copiers, leaving large amounts of data vulnerable.
- According to a report published by McAfee in March 2009, companies lost an average of \$4.6 million last year in intellectual property.
- Xerox is the only hardcopy vendor with an active security patch program. We monitor for new vulnerabilities on our MFPs, just as operating system software developers track for new viruses that could threaten their software. Security bulletins are posted on www.xerox.com/security. Customers can sign up for an RSS feed and be alerted immediately when a new bulletin and downloadable patch is posted.
- Careful design of the Embedded Fax subsystem assures complete separation between the telephone line and network fax connection on many Xerox MFPs. The Image Overwrite option electronically “shreds” information stored on the hard disk of the machines while extensive use of encryption on the disk and on the wire protects sensitive data both at rest and in transit.
- Other security features including Network Authentication allow administrators to limit access to certain users, while Secure Print and the Xerox Secure Access Unified ID System store jobs on a machine until the owner releases the document by entering a personal number, logging into a device or swiping their identification badge.

Xerox's Investment in Security

- Xerox has five research centers worldwide and spends five percent of its annual revenue on security and other critical research, development and engineering projects.
- Xerox products are designed to support standards set forth in The Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, Gramm-Leach-Bliley Act and FDA 21 CFR Part 11.

Tips

- Businesses should work with their vendor to identify their specific security needs – Xerox works directly with its customers to identify where their information resides, how it is transferred and detect the greatest areas of risk.
- Before disposing of or trading in old equipment you should check the manufacturer's product documentation to best understand the steps to wipe the machine if required.
- Customers returning a Xerox MFP that contains a hard drive should run an on-demand image overwrite before returning the machine. Xerox also offers a hard disk removal service. For a flat fee, a Xerox technician will remove the hard drive and turn it over to the customer for disposal.
- Paper is the least secure way to manage information. Look at methods to scan and digitally secure information into a trackable and securable format.
- For fax users, consider moving to electronic formats to track and secure the information. A Xerox MFP with fax forward to e-mail is a perfect way.
- Choose the right device. Often the most secure solution is a local connected device off the network or line of sight by a user.

- Devices that are hidden from view (i.e. in a copy room with nobody near the machine) increase the opportunity for employees to breach security.
- Xerox seeks independent, third-party validation of the security of its devices by participating in the International Common Criteria program for security certification. Xerox is the only vendor to include the entire device in the evaluation, not just a kit. This is important for government agencies purchasing MFPs with hard drives, like the WorkCentre 7425/7428/7435 MFPs. This certification is a great way to ensure extra protection is built into the machine. After purchasing a certified MFP, it is critical for users to enable and use all security features available to them and their machines.

Xerox Security Features

Xerox is a leader in document technology and builds a variety of features into its machines to help safeguard customers' information, including:

- **Hard Drive Removal** – On MFPs with hard drives, Xerox offers options for removal of the hard drive before the MFP is disposed of or turned in after a lease. While ultimately the customer is responsible for their data, Xerox works with customers to ensure they understand the risks associated with data when returning machines, along with providing recommendations on the most effective way to rid the hard drive of data.
- **Fax/Network Separation** – Xerox devices include a network firewall to prevent unauthorized access to a customer's system through the network connection. However, unprotected fax connections in MFPs can be an open back door into the network. Xerox devices provide complete separation of the telephone line and network fax connection.
- **Image Overwrite Option** – The Image Overwrite Security option, free on most Xerox MFPs, electronically "shreds" information stored on the hard disk(s) of devices as part of routine job processing. The electronic erasing can be performed automatically when each print job is completed, or started manually as needed.
- **Network Authentication and Authorization** – Access to scan, e-mail and fax features can be restricted by verifying network user names and passwords in network directories prior to use of these functions. Access permissions can be controlled on a per-user and per-service basis, all managed centrally at the network domain controller. Additionally, all activity is monitored and recorded in a security audit log.
- **Encryption** – All data in motion in and out of the device, as well as data stored within the device is secured with state-of-the-art encryption.
- **Secure Print** – Jobs are safely stored at the device until the owner enters a personal number to release them. This controls unauthorized viewing of documents sent to the printer.
- **Xerox Secure Access Unified ID System** – Users simply log in with a swipe of their magnetic or proximity ID card for secure access to MFP functions that need to be tracked for accounting or regulatory requirements.

Xerox Disposal Policies for MFP Hard Drives

Much like with laptops and PCs, the protection of data is ultimately the customer's responsibility and it is important to take appropriate measures to protect that information. However, Xerox considers it unacceptable that any customer data could escape once a machine has been returned to our control and the following processes are in place to ensure the greatest possible protections are in place.

- Xerox trade-ins and returns that will be remanufactured are either overwritten or reformatted. All Xerox refurb centers in North America and Mexico overwrite the hard disks.
- All Xerox trade-ins that will be disposed of are crushed and shredded.
- All competitive trade-in machines are crushed and shredded.

More Information

More information on the features or Xerox security in general is available at www.xerox.com/security.

To find out if your Xerox product contains a hard disk and comes with overwrite capability and/or disk encryption, Xerox offers a reference guide at

http://www.xerox.com/downloads/usa/en/c/cert_Xerox_Product_Security-Data_Protection.pdf

-XXX-