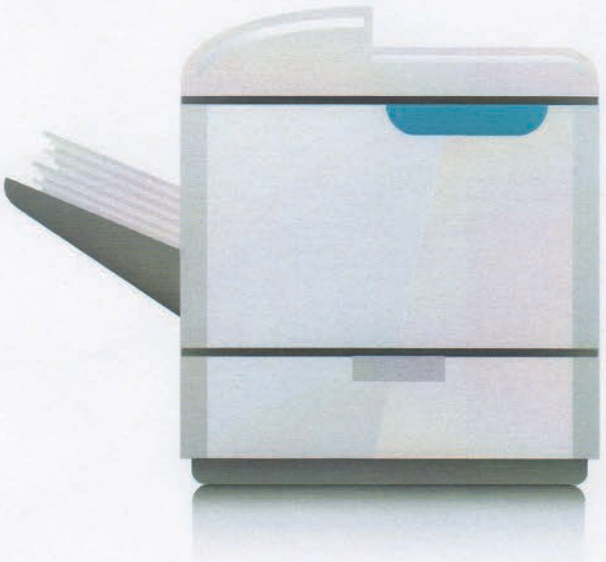
COPIER DATA SECURITY:

A GUIDE FOR BUSINESSES



FEDERAL TRADE COMMISSION | business.ftc.gov

Does your company keep sensitive data — Social Security numbers, credit reports, account numbers, health records, or business secrets? If so, then you've probably instituted safeguards to protect that information, whether it's stored in computers or on paper. That's not only good business, but may be required by law.

According to the Federal Trade Commission (FTC), the nation's consumer protection agency, your information security plans also should cover the digital copiers your company uses. If the data on your copiers gets into the wrong hands, it could lead to fraud and identity theft.

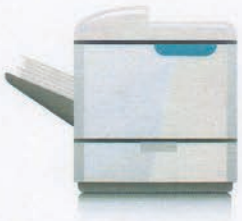
DIGITAL COPIERS ARE COMPUTERS

Commercial copiers have come a long way. Today's generation of networked multifunction devices — known as "digital copiers" — are "smart" machines that are used to copy, print, scan, fax and email documents. Digital copiers require hard disk drives to manage incoming jobs and workloads, and to increase the speed of production. But not every copier on the market is digital: generally, copiers intended for business have hard drives, while copiers intended for personal or home office use do not.

The hard drive in a digital copier stores data about the documents it copies, prints, scans, faxes or emails. If you don't take steps to protect that data, it can be stolen from the hard drive, either by remote access or by extracting the data once the drive has been removed.

Digital copiers store different types of information in different ways. For example, photocopied images are more difficult to access directly from the hard drive than documents that are faxed, scanned or printed on the copier.

THE LIFE-CYCLE OF A COPIER



Copiers often are leased, returned, and then leased again or sold. It's important to know how to secure data that may be retained on a copier hard drive, and what to do with a hard drive when you return a leased copier or dispose of one you own.

It's wise to build in data security for each stage of your digital copier's life-cycle: when you plan to acquire a device, when you buy or lease, while you use it, and when you turn it in or dispose of it.

BEFORE YOU ACQUIRE A COPIER:

Make sure it's included in your organization's information security policies. Copiers should be managed and maintained by your organization's IT staff. Employees who have expertise and responsibility for securing your computers and servers also should have responsibility for securing data stored on your digital copiers.

WHEN YOU BUY OR LEASE A COPIER:

Evaluate your options for securing the data on the device. Most manufacturers offer data security features with their copiers, either as standard equipment or as optional add-on kits. Typically, these features involve encryption and overwriting.

Encryption is the scrambling of data using a secret code that can be read only by particular software. Digital copiers that offer encryption encode the data stored on the hard drive so that it cannot be retrieved even if the hard drive is removed from the machine.

Overwriting — also known as file wiping or shredding — changes the values of the bits on the disk that make up a file by overwriting existing data with random characters. By overwriting the disk space that the file occupied, its traces are removed, and the file can't be reconstructed as easily.

Depending on the copier, the overwriting feature may allow a user to overwrite after every job run, periodically to clean out the memory, or on a preset schedule. Users may be able to set the number of times data is overwritten — generally, the more times the data is overwritten, the safer it is from being retrieved. However, for speed and convenience, some printers let you save documents (for example, a personnel leave slip) and print them straight from the printer hard drive without having to retrieve the file from your computer. For copiers that offer this feature, the memory is not overwritten with the rest of the memory. Users should be aware that these documents are still available.

Overwriting is different from deleting or reformatting. Deleting data or reformatting the hard drive doesn't actually alter or remove the data, but rather alters how the hard drive finds the data and combines it to make files: The data remains and may be recovered through a variety of utility software programs.

Yet another layer of security that can be added involves the ability to lock the hard drives using a passcode; this means that the data is protected, even if the drive is removed from the machine.

Finally, think ahead to how you will dispose of the data that accumulates on the copier over time. Check that your lease contract or purchase agreement states that your company will retain ownership of all hard drives at end-of-life, or that the company providing the copier will overwrite the hard drive.

WHEN YOU USE THE COPIER:

Take advantage of all its security features. Securely overwrite the entire hard drive at least once a month.

If your current device doesn't have security features, think about how you will integrate the next device you lease or purchase into your information security plans. Plan now for how you will dispose of the copier securely. For example, you may want to consider placing a sticker or placard on the machine that says: "Warning: this copier uses a hard drive that must be physically destroyed before turn-in or disposal." This will inform users of the security issues, and remind them of the appropriate procedures when the machine reaches the end of its usable life.

In addition, your organization's IT staff should make sure digital copiers connected to your network are securely integrated. Just like computers and servers that store sensitive information, networked copiers should be protected against outside intrusions and attacks.

WHEN YOU FINISH USING THE COPIER:

Check with the manufacturer, dealer, or servicing company for options on securing the hard drive. The company may offer services that will remove the hard drive and return it to you, so you can keep it, dispose of it, or destroy it yourself. Others may overwrite the hard drive for you. Typically, these services involve an additional fee, though you may be able to negotiate for a lower cost if you are leasing or buying a new machine.

One cautionary note about removing a hard drive from a digital copier on your own: hard drives in digital copiers often include required firmware that enables the device to operate. Removing

and destroying the hard drive without being able to replace the firmware can render the machine inoperable, which may present problems if you lease the device. Also, hard drives aren't always easy to find, and some devices may have more than one. Generally, it is advisable to work with skilled technicians rather than to remove the hard drive on your own.

FOR MORE INFORMATION

To learn more about securing sensitive data, in general, read *Protecting Personal Information: A Guide for Business* at **ftc.gov/infosecurity**.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace and to provide information to businesses to help them comply with the law. To file a complaint or to get free information on consumer issues, visit **ftc.gov** or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a new video, *How to File a Complaint*, at **ftc.gov/video** to learn more. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

OPPORTUNITY TO COMMENT

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to **sba.gov/ombudsman**.

PROTECTING SENSITIVE INFORMATION: YOUR LEGAL RESPONSIBILITY

The FTC's standard for information security recognizes that businesses have a variety of needs and emphasizes flexibility: Companies must maintain reasonable procedures to protect sensitive information. Whether your security practices are reasonable depends on the nature and size of your business, the types of information you have, the security tools available to you based on your resources, and the risks you are likely to face.

Depending on the information your business stores, transmits, or receives, you also may have more specific compliance obligations. For example, if you receive consumer information, like credit reports or employee background screens, you may be required to follow the Disposal Rule, which requires a company to properly dispose of any such information stored on its digital copier, just as it would properly dispose of paper information or information stored on computers. Similarly, financial institutions may be required to follow the Gramm-Leach-Bliley Safeguards Rule, which requires a security plan to protect the confidentiality and integrity of personal consumer information, including information stored on digital copiers.

business.ftc.gov
November 2010