

Protecting Personally Identifiable Information In The Workplace: A Study Guide*

SAMPLED

**Protecting Personally Identifiable Information
In The Workplace: A Study Guide**

Top Level Steps Overview (TL)

TL Step #	Action	Start Date	Finished Date	N/A
A	Board Of Directors / Owner / or CEO have mandated in writing the implementation of a Personally Identifiable Information Data Security Policy			
B	A senior level employee, or business owner, has been designated, in writing, as the entity's Data Security Officer (DSO)			
C	All data acquired for business transactions and employment purposes has been inventoried and risk assessment of that data has been evaluated			
D	Data acquired has been reduced to only that which is required and only for as long it is required			
E	Data security procedures, for both physical and electronic formats, have been evaluated, streamlined, and access to it has been protected from non-users			
F	Disposal procedures have been assigned to all data types inventoried in step C			
G	Continuous and routine evaluation procedures have been established to monitor the effectiveness of all data management procedures, noted in steps C, D, E, & F, for all current and for future data processes introduced to meet changing business requirements			
H	A written personally identifiable information data security and privacy policy has been completed and implemented			
I	All employees have been trained to understand the personally identifiable information data security and privacy policy and their role in adhering to the policy and the enforcement rules of the policy for compliance			
J	New employee training on the entity's personally identifiable information data security and privacy policy has been incorporated into their orientation program			
K	All employees have been trained as to their personal responsibility to monitor their own personal information for suspicious use and report immediately any such use that affects the integrity of the entity's personally identifiable information data security and privacy policy			
L	**** Continues in actual 39 page Study Guide ****			

Protecting Personal Information: Five Steps for Business

by Lesley Fair

What's in your file cabinet right now? Tax records? Payroll information? And what's on your computer system? Financial data from your suppliers? Credit card numbers from your customers? To a busy marketer, those documents are an everyday part of doing business. But in the hands of an identity thief, they're tools for draining bank accounts, opening bogus lines of credit, and going on the shopping spree of a lifetime — at the expense of your company, your employees, and the customers who trust you.

Sophisticated hack attacks make the headlines, but many security breaches could be prevented by commonsense measures that cost companies next to nothing. That's why the Federal Trade Commission (FTC) has published [*Protecting Personal Information: A Guide for Business*](#), a plain-language handbook with practical tips on securing sensitive data. The specifics depend on the size of your company and the kind of information you have, but the basic principles remain the same. Whether you work for a multinational powerhouse with branches around the world or a start-up based in a home office, a sound information security plan is built on these five key practices:

- **Take stock.** Know what personal information you have in your files and on your computer. Understand how personal information moves into, through, and out of your business and who has access — or could have access to it.
- **Scale down.** Keep only what you need for your business. That old business practice of holding on to every scrap of paper is “so 20th century.” These days, if you don't have a legitimate business reason to have sensitive information in your files or on your computer, don't keep it.
- **Lock it.** Protect the information you keep. Be cognizant of physical security, electronic security, employee training, and the practices of your contractors and affiliates.
- **Pitch it.** Properly dispose of what you no longer need. Make sure papers containing personal information are shredded, burned, or pulverized so they can't be reconstructed by an identity thief.
- **Plan ahead.** Draft a plan to respond to security incidents. Designate a senior member of your team to create an action plan before a breach happens.

Get your copy of *Protecting Personal Information: A Guide for Business* at www.ftc.gov/infosecurity. While you're there, download copies for your IT manager, your human resources department, your sales staff, and anyone else who comes in contact with customer or employee information.

Lesley Fair is an attorney in the FTC's Bureau of Consumer Protection who specializes in business compliance.

FTC Website: <http://www.ftc.gov/bcp/edu/pubs/articles/art01.shtm>

**Protecting Personally Identifiable Information
In The Workplace: A Study Guide
Take Stock**

Take Stock: Conducting a Data Security Audit in Your Office

by Lesley Fair

It may mean one thing on TV, but to savvy business executives, “CSI” should stand for Carefully Secure Information. Every company has an obligation to its customers, affiliates, and employees to safeguard sensitive data. As outlined in the Federal Trade Commission’s new handbook, ***Protecting Personal Information: A Guide for Business***, one step of the process is to “Take Stock” — conduct a CSI-style “forensic audit” of your information practices.

Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has — or could have — access to it is essential to assessing security vulnerabilities. Whether you’re a industry giant or a lean-and-mean one-person shop, here are some tips on conducting your own “CSI” investigation:

- **Secure the scene.** Inventory all file cabinets, computers, flash drives, disks, and other equipment to find out where your company stores sensitive data. Don’t forget about laptops, employees’ home offices, cell phones, and email attachments. No security audit is complete until you check everywhere sensitive data might be stored.
- **Look for footprints.** Track personal information through your business by talking with your technology staff, human resources office, accounting personnel, and outside service providers. Get a complete picture of who sends your company sensitive data. Do you get it from customers? Call centers? Credit card companies? Banks or other financial institutions? Affiliates and contractors?
- **Check the doors.** How does sensitive data come in to your company? From your website? Via email? Through the mailroom? What kind of information is collected at each entry point? Customers’ credit card, debit, or checking account numbers? Sensitive health or financial data?
- **Dust for fingerprints.** Who has — or could have — access to the information? Which of your employees has permission to look at sensitive data? Could anyone else get a hold of it? What about vendors who supply and update software you use to process credit card transactions? Contractors running your call center, distribution, or fulfillment operations?
- **Protect key evidence.** Different types of data present varying risks. Pay particular attention to how you keep personally identifiable information like Social Security numbers; credit card, debit, checking account, or financial information; and other sensitive data that could facilitate fraud or identity theft if it fell into the wrong hands.

Get your copy of ***Protecting Personal Information: A Guide for Business*** at www.ftc.gov/infosecurity.

Lesley Fair is an attorney in the FTC’s Bureau of Consumer Protection who specializes in business compliance. FTC website: <http://www.ftc.gov/bcp/edu/pubs/articles/art02.shtm>

**Protecting Personally Identifiable Information
In The Workplace: A Study Guide
Take Stock (TS)**

TS Step #	Action	Start Date	Finished Date	N/A
1.00	<p>Take Stock: Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has - or could have - access to it is essential to assessing security vulnerabilities. You can determine the best ways to secure the information only after you've traced how it flows.</p>	Intro	Statement	N/A
1.10	Form protecting personally identifiable information (PII) process teams based on a cross departmental basis that share PII from input through to disposal			
1.20	<p>Inventory:</p> <ul style="list-style-type: none"> - all computers, - laptops, - flash drives, - disks, - home computers, - Any other equipment to find out where your company stores sensitive data. - _____ - _____ <p>Also inventory the information you have by type and location:</p> <ul style="list-style-type: none"> - File cabinets, - Storage rooms, - computer systems - _____ - _____ <p>These are a start, but remember: your organization receives personal information in a number of ways:</p> <ul style="list-style-type: none"> - through websites, - from contractors, - from call centers, - And the like: _____ <p>What about information saved on:</p> <ul style="list-style-type: none"> - laptops, - employees' home computers, - flash drives, 			

	<ul style="list-style-type: none"> - cell phones - and _____ - _____ <p>No inventory is complete until you check everywhere sensitive data might be stored.</p>			
1.21	Schedule all forms on an electronic worksheet (Excel, Lotus, etc) and segregate between those that contain personally identifiable information (PII) and those that do not contain any PII.			
1.22	Create a worksheet for each PII document (paper form or electronic screens) (See example of wksh1)			
1.23	List all fields contained on the PII document down the left column (See example of wksh2)			
1.24	Review to determine PII fields and designate all sensitive information fields: Different types of information present varying risks. Pay particular attention to how you keep personally identifiable information: Social Security numbers, credit card or financial information, and other sensitive data. That's what thieves use most often to commit fraud or identity theft. (See example of wksh2)			
1.30	Track personal information through your business by talking with your sales department, information technology staff, human resources office, accounting personnel, and outside service providers. Get a complete picture of:			
1.31	<p>Who sends sensitive personal information to your organization?</p> <ul style="list-style-type: none"> - Do you get it from customers? - Credit card companies? - Banks or other financial institutions? - Credit bureaus? - Other businesses? 			
1.32	<p>How does your business receive personal information?</p> <ul style="list-style-type: none"> - Does it come to your business through a website? - By email? - Through the mail? - Is it transmitted through cash registers in stores? 			
1.33	Determine exit points and methods PII forms uses to exit the entity (such as by physical carrier, electronic transmission including email, data storage devices – tapes, drives, or other physical electronic mediums)			
1.34	Determine the process flow (cross departmental) of the all PII forms throughout the entity on a high end for further study in 1.35 below.			
1.35	**** Continues in actual 39 page Study Guide ****			

Lock It: Protecting Your Office from Info Thieves

by Lesley Fair

Sometimes the key to data security is an old-fashioned lock. *Protecting Personal Information: A Guide for Business*, a new handbook from the Federal Trade Commission, offers advice on protecting your customers and employees by securing sensitive data. One important tip: Lock it — Protect the information that you keep.

- **Lock, stock — or peril.** Computer defenses can be critical, but when it comes to protecting personal information, don't forget "old school" physical security, too. Discourage light-fingered passersby by making sure every employee has a secure drawer or locker. Centralize sensitive paperwork and limit access to employees with a legitimate business need. Remind them not to leave documents out when they step away from their desks. Shipping data offsite? Consider encrypting it and using a mailing method that will allow you to track the package en route.
- **Barbarians at the gate.** Viruses, spyware, and other invaders will attack an unprotected computer in just seconds. Your tech staff has sophisticated defensive tools at their disposal, but be sure to remind your employees that electronic security is everybody's business. Use strong passwords (the longer, the better) and require your staff — including the ones who wreathe their computer screens with passwords scrawled on sticky notes — to store them securely and change them regularly. Ask your IT people to install an intrusion detection system to tip them off to network breaches. Monitor incoming and outgoing traffic for higher-than-average use at unusual times of the day. Check expert resources like www.sans.org and your software vendors' websites for alerts about the latest vulnerabilities and vendor-approved patches.
- **We have met the enemy and he is us.** Hackers certainly pose a threat, but sometimes the biggest risk to a company's security is an otherwise conscientious employee who hasn't learned the basics about protecting personal information. Create a culture of security by implementing a regular schedule of employee training. Make it clear to new staff that abiding by your company's data security plan is an essential part of their job. Make account data, credit card numbers, or other sensitive information available only on a "need to know" basis. Have a procedure in place for making sure that workers who leave your employ or move to another part of the business no longer have access to off-limits information.
- **Trust, but verify.** That Cold War phrase should describe your approach to the security practices of your contractors and service providers. Before outsourcing any of your business functions — payroll, web hosting, call center operations, data processing, fulfillment, and the like — investigate the company's data security practices and compare their standards to your own. Make sure your expectations and requirements are spelled out in the contract and build in a way for you to monitor their performance. Insist that contractors and service providers notify you immediately if they experience a security incident, even if it may not have led to an actual compromise of your data.

Get your copy of *Protecting Personal Information: A Guide for Business* at www.ftc.gov/infosecurity.

Lesley Fair is an attorney in the FTC's Bureau of Consumer Protection who specializes in business compliance. FTC Website: <http://www.ftc.gov/bcp/edu/pubs/articles/art04.shtm>

**Protecting Personally Identifiable Information
In The Workplace: A Study Guide**

Lock It (LI)

LI Step #	Action	Start Date	Finished Date	N/A
3.0	Lock It: What's the best way to protect the sensitive personally identifiable information you need to keep? It depends on the kind of information and how it's stored. The most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers	Intro	Statement	N/A
3.10	Physical Security: Many data compromises happen the old-fashioned way - through lost or stolen paper documents. Often, the best defense is a locked door or an alert employee			
3.11	Store paper documents or files, as well as CDs, floppy disks, zip drives, tapes, and backups containing personally identifiable information in a locked room or in a locked file cabinet. - Limit access to employees with a legitimate business need. - Control who has a key, and the number of keys			
3.12	- Require that files containing personally identifiable information be kept in locked file cabinets except when an employee is working on the file. - Remind employees not to leave sensitive papers out on their desks when they are away from their workstations. - Post signs around work areas that need to be cleared when not in use especially during breaks or overnight			
3.13	**** Continues in actual 39 page Study Guide ****			

Other entire sections not shown in this Sample document include:

- **Employee Training**
- **Scale down.**
- **Pitch it.**
- **Plan ahead.**
- **Lap top computer (and other portable electronic device issues).**
- **F.A.C.T.A. Red Flags Law.**