



insert BGA logo here

# The Brokerage Industry Guide For Securing Confidential Information

*Authors:*

*NAILBA Technology Committee*

insert BGA contact information here

© February 2008, National Association of Independent Life Brokerage Agencies, Fairfax, Virginia.

Disclaimer: This information is provided solely for educational and informational purposes. It is not intended to constitute legal advice. Readers should obtain legal advice specific to their company and circumstances in connection with each of the topics addressed

## Table of Contents

Executive Summary .....	3
Information Privacy Laws and Regulations .....	4
Recognizing Confidential Information .....	5
Information Asset Classification .....	5
The Brokerage Industry Guide for Securing Confidential Information .....	6
General Guidelines .....	6
Password Security.....	6
Password Guidelines .....	6
Follow these guidelines for establishing and maintaining secure passwords: .....	6
Electronic Devices/Media .....	6
Servers.....	6
External Threats .....	7
Internal Threats.....	7
General Server Security Guidelines .....	7
Workstations and Laptops .....	7
Laptop Physical Security.....	8
Network Security .....	8
Wireless Network Security.....	9
PDAs/Mobile Phones .....	9
USB and FireWire Portable Storage Devices .....	9
Security Options .....	9
Backup Tapes and Media.....	9
Third-Party Vendors.....	9
Physical Media: Hard-Copy Paper .....	9
Other Considerations for Securing Confidential Information .....	10
New Federal Rule for Disposing of Consumer Report Information.....	10
What Information Does the Disposal Rule Cover?.....	10
What Is Considered “Proper” Disposal? .....	11
In Case of a Security Breach .....	11
Breach of Security Notification Laws .....	11
Relationship to Other Laws .....	12
Case Studies and Important References .....	12
Appendix: Information Security Checklist.....	13

## Executive Summary

Information is a vital business asset. A company has an ethical and professional requirement to securely serve its customers, interact with its business partners and respect the confidence placed upon it by these persons and entities. As a result, the underlying information infrastructure that drives a company's business must be secured.

A company must take all appropriate action to secure its information in all forms (e.g., spoken, written, electronic, audio, video, magnetic, microfiche, and email). Information produced or residing in your systems may be deemed to be the property of your firm and must be secured as such.

In the office, the increasing power and use of IT has spurred a virtually non-stop exchange of electronic data and documents among co-workers, business partners and customers.

Many of us rely on mobile computing devices. Wireless accessories have become pervasive in our industry, especially laptop computers, PDAs, USB memory (i.e., "thumb drives") and smart phones (mobile phones with advanced communication, storage and processing capabilities). These devices offer convenience and ease of use. They also include unacknowledged risks.

Information security is the ongoing process of exercising due care and due diligence to secure information and information systems from unauthorized access, use, disclosure, destruction, modification or disruption. The never ending process of information security involves ongoing training, assessment, protection, monitoring and detection, incident response and repair, documentation and review.

This document may be used as a checklist concerning the main risks associated with using these devices in your office and public areas. It proposes both short- and long-term approaches to securing confidential information.

# Information Privacy Laws and Regulations

The Gramm-Leach-Bliley Act (GLB), also known as the Financial Services Modernization Act, is a federal law, which includes a privacy provision requiring that financial services companies have a customer privacy policy and notify customers of that policy at time of application and annually every year thereafter. The state and federal agencies regulating financial institutions must apply the GLB privacy provisions regarding the collection, use and disclosure of non-public customer information to those institutions that they have authority to regulate. As a result, there are numerous regulations issued by different state and federal agencies that apply privacy provisions to financial institutions. (See <http://www.ftc.gov/privacy/glbact/glbsub1.htm>.)

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996. The purpose of HIPAA is to apply privacy policy for securing the confidentiality and security of medical information of all affected policyholders and new applicants. This law ensures continuity of health care coverage for individuals changing jobs; regulates the management of health information; seeks to simplify the administration of health insurance; and aims to combat waste, fraud and abuse in health insurance and health care. A series of rules or administrative regulations derived from the HIPAA law have been developed and issued by the Department of Health and Human Services (HHS) to implement these requirements. These regulations will impact all health care organizations that create, store or transmit health care data.

This document presents an overview of three key HIPAA regulations:

- HIPAA Privacy
- HIPAA Administrative Simplification
- HIPAA IT Security

Companies must develop and implement physical, administrative and technical safeguards to achieve the following goals:

- Ensure the security and confidentiality of customer records and information
- Secure against any anticipated threats or hazards to the security or integrity of such information
- Secure against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer

Information assets should be risk-assessed and classified so that they are appropriately secured based on their value and the degree of harm that could result from unauthorized disclosure, misuse, modification, destruction or non-availability or as required by legislation. Information assets should be consistently secured with the appropriate risk management techniques and standardized controls in a cost-effective and timely manner that will vary according to the asset value and the risk. (See <http://www.hhs.gov/ocr/hipaa>.)

# Recognizing Confidential Information

Information is considered confidential when it is personal to an individual or entity and is not available publicly. The following table presents a partial list of common types of confidential information.

Account numbers	Email messages	Plan beneficiary number
Asset distribution upon death	Email addresses, street addresses and phone numbers	Policy number (if used in combination with full name or other identifiable information)
Bank account number	Estate holdings and mortgage amounts	Religious affiliation
Credit card number	Family information like ownership of assets	Retirement plans
Credit history	Individual Taxpayer Identification Number (ITIN)	Salary
Criminal conviction	Medical conditions	Sexual behavior/lifestyle
Debit card number	Medical histories and blood test results	Social Security Number
Driver's license number	Medications	Tax ID
Drugs, therapies, or medical products or equipment used	Net worth	Tax returns

# Information Asset Classification

Information assets should be classified and have a designated business owner; often the head of a business unit area is considered the owner. The business owner is responsible for the information asset from the time it is created until it is disposed. The following table outlines various types of information assets and how they might be safeguarded.

Classification	Brief Description	Example	Examples of Possible Safeguards
Public	<b>Information officially released by the company for unrestricted public disclosure.</b> While confidentiality is often low, the availability and integrity of this data is crucial.	This includes information approved for public release, such as the information available on public websites, as well as information released to the press.	<ul style="list-style-type: none"> <li>• Usage of data: limited to employees and authorized users</li> <li>• Transmission: no special requirements</li> <li>• Storage: no special requirements</li> <li>• Disposal: can be recycled</li> </ul>
Internal	<b>Assets for which unauthorized disclosure, access, modification or destruction, whether the result of inadvertent or deliberate actions, could have a limited adverse impact on business.</b> Confidentiality is usually considered medium while availability and integrity rank from low to high.	This is non-public data, which typically includes organizational charts, employee telephone lists, policy and process documentation, and operational communications.	<ul style="list-style-type: none"> <li>• Usage of data: access limited to read-only</li> <li>• Transmission: no special requirements</li> <li>• Storage: office locations and password-secured systems or files</li> <li>• Disposal: shredded or erased</li> </ul>
Restricted	<b>Assets for which unauthorized disclosure, access, modification or destruction, whether the result of inadvertent or deliberate actions, could have a significant impact to employees, business partners or the company as a whole.</b> Restricted assets can often be distinguished from internal assets in both size (e.g., total cost) and scope (number of business units affected) of the potential impact. Confidentiality, integrity and availability are generally high for these assets.	This can include business, marketing and sales plans, and other information that could be used as harmful competitive intelligence.	<ul style="list-style-type: none"> <li>• Usage of data: access limited to those with operational requirements</li> <li>• Transmission: encryption on public networks</li> <li>• Storage: locked office, filing cabinets and password-secured systems or files</li> <li>• Disposal: shredded or degaussed (removal of magnetic information)</li> </ul>
Regulated	<b>Assets for which unauthorized disclosure, access, modification or destruction, whether the result of inadvertent or deliberate actions, could have regulatory, legal or statutory repercussions.</b> Confidentiality, integrity and availability are generally very high for these assets.	This can include all personal medical information and privacy-related, non-public personal information, as well as company earnings information, transaction information or other financial data.	<ul style="list-style-type: none"> <li>• Same as Restricted, with additional controls as needed to satisfy legal, regulatory or statutory requirements</li> </ul>

All users have a responsibility to safeguard information in all forms, from its creation through its useful life until its disposal.

# The Brokerage Industry Guide for Securing Confidential Information

## General Guidelines

At a minimum, your information security policy should follow these guidelines:

- Only share sensitive information with those who need it to perform their jobs.
- Do not discuss client information in public places.
- Confirm the identity of anyone requesting client information.
- Maintain strict physical electronic and procedural safeguards to secure non-public information.
- Shorten policyholder names to first initial and last name.
- Truncate certain account numbers (e.g., driver's license number, bank account number, credit card number and debit card number).
- Truncate or encrypt confidential information.

## Password Security

Almost all confidential information is hidden behind some type of password authentication. One of the most overlooked security holes in any network or systems is password security. Failure to adequately secure user names and passwords could result in a security breach.

### *Password Guidelines*

*Follow these guidelines for establishing and maintaining secure passwords:*

- Passwords should be at least seven characters long. The more characters in a password, the longer it takes to crack it.
- Passwords should contain at least one letter and at least one digit.
- If compatible, passwords should contain both uppercase and lowercase letters, as well as at least one punctuation mark or other special character.
- Passwords should not be based on any part of the user's name or login ID.
- Passwords should not be based on any dictionary word, in any language.
- Users should never share their passwords with friends or coworkers.
- Users should never write their passwords down.
- Passwords should be changed at least every 90 days, preferably more frequently.
- Never use the same user names and passwords when logging into multiple systems or websites.
- Users should never reuse old passwords.

## Electronic Devices/Media

### **Servers**

There are basically two sources of risk to your production servers: external threats and internal threats.

**External threats** are those sources that originate outside of your network and are trying to gain access to your network. The most common access point is your organization's Internet connection. However, often overlooked access points are modems and modem pools used for dialup users, as well as unsecured wireless access points. Users with access to the Internet pose a serious security risk to companies. Users unknowingly accessing malicious websites or downloading malicious files may compromise their computers and provide a back door to your network and servers.

**Internal threats** are those sources that already have access to your network. Many of the security breaches that occur every year come from internal users who already have access to the network. Internal threats can be divided into several categories:

- **Corporate espionage.** Employees may steal data for a competitor or to start their own competing business.
- **Malicious and/or disgruntled employee.** Current or recently terminated employees may wish to do harm to the company.
- **Unintentional breaches.** Risks posed by employees include installing unauthorized software, browsing malicious websites, opening virus infected emails or falling for social engineering attacks.
- **Non-employees with network access.** Temp workers, interns, visitors, guests and janitorial service personnel may have internal access to your network, whether authorized or not.

### **External Threats**

Firewalls are your first line of defense from external threats. Any network that is connected to the Internet should have a firewall securing it. Firewalls work by blocking access from the outside to any internal applications and resources. If an application such as a web server or email server has to be accessible from the Internet, then a firewall will offer minimal security protection for those applications. In those cases, the security burden is on the application vendor to ensure that the application is secure.

Applications that are accessible from the Internet should be housed on servers located on an isolated network called a DMZ. By isolating your Internet-facing applications, you reduce the risk of your network being compromised should your application server be compromised.

To reduce the risk of malicious application such as viruses and Trojan horses being sent via email, anti-virus and anti-spam gateways should be used before an email reaches your mail server.

Use a web-filtering solution to limit Internet access for your employees. By using such a solution, you can reduce your risk of employees accessing and downloading malicious content from websites.

### **Internal Threats**

Disable and remove all unused server applications. Many server operating systems come with several server applications that are installed by default, which may be a possible security risk. If those applications are not used, they should be removed.

Servers should be stored in a secure room with controlled access. In addition, always enable firewall services on your servers to restrict the ports that are accessible on your internal network.

### **General Server Security Guidelines**

Follow these guidelines for general server security:

- Always use strong passwords to secure server assets.
- Restrict administrative and/or root access to a limited number of personnel within your office.
- Always disable or remove unused accounts, services and software from your server systems.
- For file shares and applications, always set permissions to restrict access to only those who need it.
- Never use root or domain administrator accounts to run installed applications and services. Always create new accounts for each application or service with limited access to prevent malicious users from controlling your servers by exploiting security vulnerabilities within an installed application or service.
- Keep all server operating systems and applications patched and up-to-date.
- An anti-virus application should be installed on your servers to prevent viruses from being loaded or copied to the server.

### **Workstations and Laptops**

- Always lock your workstation before leaving it unattended.

- Log off all computer systems when you are done using them.
- All workstations and laptops should be password-secured with complex passwords.
- Use port-locking software to secure USB and infrared ports. Port-locking software requires a user to enter a password before being able to transfer information via the secured ports.
- Keep operating systems and other applications patched and up to date to reduce the risk of security vulnerabilities. All applications on the workstation or laptop should be patched and updated from the appropriate vendor's website.
- Antivirus software and spyware-detection software should be installed and regularly updated on the workstation or laptop. The workstation or laptop also should be configured with a personal firewall and intrusion detection system to prevent unauthorized access and malicious code in the system.
- All workstation or laptops should have an encrypted file system. There are two types of encryption solutions; the best encryption solutions available use a combination of both technologies:
  - **Disk-Level Encryption.** When a computer is shut down, all the contents of a hard disk are encrypted. When the computer is turned on, a password must be entered in order to decrypt the disk. One of the limitations of this type of encryption is that once the computer is up and running, all the files on the hard drive are unencrypted. If a malicious user is able to access your computer remotely, that user would have access to all files on your computer.
  - **File-Level Encryption.** Individual folders and documents can be encrypted. This solution secures the information regardless of whether the computers are on or off. The downside is that not all files on the hard disk can be encrypted. For example, if you encrypt the operating system directories, then you may no longer be able to boot the operating system. Another problem with this solution is that it is up to the user to save information in an encrypted directory in order for it to be secured.
- Use secure, time-tested operating systems on your workstation or laptop that have high security incorporated.
- Disable the display of last logged in user name in the login dialog box.
- Perform data backups on a regular basis.
- Disable unnecessary user accounts, and rename the administrator account.

### **Laptop Physical Security**

Due to the portability of these computer systems, there are several potential security risks that need to be addressed.

Cables and hardwired locks to secure a laptop to a fixed piece of furniture can reduce the risk of a laptop being stolen. The disadvantage to locks and cables is that the laptop must be attached to an object that cannot be easily dismantled or destroyed. In addition, this solution does not secure removable items such as hard drives and CD-ROM bays.

Laptop safes can be used to secure laptops and add additional advantages over security cables. A laptop safe secures the entire laptop and all of its removable items, such as hard drives and CD-ROM bays.

Follow these additional guidelines for increased physical security:

- Never leave a laptop unattended in public places.
- Never leave a laptop exposed in your car.
- Laptops should be carried as hand luggage while traveling.
- Sensitive information displayed on the screen should not be displayed in public places.

### **Network Security**

- Use firewalls to restrict access to your network from the Internet or other external network.
- Use VPN technology to access corporate networks from remote locations when using unsecured networks such as the Internet.

## **Wireless Network Security**

Wireless networks are one of the greatest security threats to your business. If a wireless network is left unsecured, anyone with line of sight to that network can potentially access it.

- Enable WEP/WPA encryption on all wireless networks. Use at least 128-bit encryption when configuring your network.
- Enable available security features. Embedded security features are often times disabled by default for wireless devices such as routers and access points.
- Disable SSID broadcasts. By disabling SSID broadcasts, users or potential intruders will not be able to select your wireless network from a list. Users will have to know the SSID in order to connect to your network.
- Define a complex SSID naming convention. Do not use default SSID names. Also, don't use SSID names that are identifiable to your company.

## ***PDA's/Mobile Phones***

- Always password-secure mobile devices.
- All sensitive data that is stored on the device, including removable memory cards, should be encrypted.
- All sensitive data should be encrypted before being transmitting wirelessly.
- Never leave a PDA unattended in a public place.
- Sync and backup data regularly.
- Only sync to a computer that has up-to-date software patches and anti-virus software.

## ***USB and FireWire Portable Storage Devices***

USB and FireWire portable storage devices pose three kinds of threats:

- They allow users to bypass perimeter defenses such as firewalls and anti-virus solutions, creating a back door to your network for malicious programs such as viruses.
- These devices allow employees and intruders to easily remove sensitive information from the premises.
- These devices can easily be lost or stolen. If left unencrypted, the information can easily be retrieved.

## **Security Options**

- **Disable USB and FireWire ports.** This solution can be implemented easily but may cause problems if your users' computers require the use of these ports for peripherals such as keyboards and mice.
- **Encrypt all portable storage devices.** Software solutions are available that allow users to encrypt the data that is stored on a USB or FireWire removable storage device. These solutions only secure the data on the portable devices and do not prevent access to the data via the USB and FireWire ports.

## ***Backup Tapes and Media***

- Backup tapes and media should always be stored in a secure location.
- All backup tapes and media should be both password-secured and encrypted to secure the data should the media be lost or stolen.

## ***Third-Party Vendors***

Application service providers and Internet service providers (e.g., email and web servers) require service providers to secure the confidentiality of non-public information shared with them.

## ***Physical Media: Hard-Copy Paper***

- Dispose of confidential document in shredder bins.

- Remove customer information from fax, photocopier and scanner machines.
- Lock up documents in file room or cabinets.
- Secure documents when sending to other areas inside or outside the company.

## Other Considerations for Securing Confidential Information

An unscrupulous client or prospective client could snatch a sheaf of applications without notice. It could be hours or even days before the theft is noticed. Using the data on the applications as the basis for identify theft, this client could have gained access to the financial accounts of applicants with tremendous potential liability on the part of the agency and/or agent.

To prevent confidential information from falling into the wrong hands (or being seen by the wrong eyes), establish strict guidelines for the employee handling of all confidential documents. Employee work manuals and initial training should emphasize the urgency of maintaining the privacy of all confidential documents. In addition, the following steps should be taken to assure complete document security:

- When employees handle confidential documents of any type, supervisors should establish a workflow for the documents. Employees should know where documents should be taken or stored when completed. Do not make employees guess what to do with confidential information. Store paper documents such as checks and documents containing confidential information in a locked and secure location. Drawers, storage boxes, file folders, lock boxes or other storage containers should be readily accessible for all confidential documents.
- Employees should never handle confidential documents when their attention is divided (e.g., taking employment applications while checking out customers or answering phones).
- Ideally confidential information should not be faxed in to the store or business. When fax must be used for this type of information, the fax machine should be in a secure area, such as an inner office. An unattended fax machine in an area open to customers and unauthorized employees is an invitation to theft.
- Confidential documents should not be let off the business premises. Credit applications and APS's should be kept onsite if possible.
- When confidential documents are discarded, never toss them into a wastebasket or dumpster. Shred or burn them. The individual or company handling the destruction should sign, date and notarize the process.

## New Federal Rule for Disposing of Consumer Report Information

In an effort to secure the privacy of consumer information and reduce the risk of fraud and identity theft, a new federal rule is requiring businesses to take appropriate measures to dispose of sensitive information derived from consumer reports.

Any business or individual who uses a consumer report for a business purpose is subject to the requirements of the Disposal Rule. This rule requires the proper disposal of information in consumer reports and records to secure against "unauthorized access to or use of the information." The Federal Trade Commission, the nation's consumer protection agency, enforces the Disposal Rule.

According to the Federal Trade Commission (FTC), the standard for the proper disposal of information derived from a consumer report is flexible and allows the organizations and individuals covered by the Disposal Rule to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods and changes in technology.

Although the Disposal Rule applies to consumer reports and the information derived from consumer reports, the FTC encourages those who dispose of any records containing a consumer's personal or financial information to take similar protective measures. The Disposal Rule applies to all different levels, from carriers to BGAs to the agents selling the insurance.

## What Information Does the Disposal Rule Cover?

The Disposal Rule applies to consumer reports or information derived from consumer reports. The Fair Credit Reporting Act defines the term "consumer report" to include information obtained from a consumer reporting company that is used, or expected to be used, in establishing a consumer's eligibility for credit, employment or insurance, among other

purposes. Credit reports and credit scores are consumer reports, and so are reports businesses or individuals receive with information relating to employment background, check-writing history, insurance claims, residential or tenant history, or medical history.

## What Is Considered “Proper” Disposal?

The Disposal Rule requires disposal practices that are reasonable and appropriate to prevent the unauthorized access to or use of information in a consumer report. For example, reasonable measures for disposing of consumer report information could include establishing and complying with policies to complete the following guidelines:

- Burn, pulverize or shred papers containing consumer report information so that the information cannot be read or reconstructed.
- Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed.
- Conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Disposal Rule; due diligence could include the following:
  - Reviewing an independent audit of a disposal company’s operations and/or its compliance with the Disposal Rule
  - Obtaining information about the disposal company from several references
  - Requiring that the disposal company be certified by a recognized trade association
  - Reviewing and evaluating the disposal company’s information security policies or procedures

The FTC says that financial institutions that are subject to both the Disposal Rule and the GLB Safeguards Rule should incorporate practices dealing with the proper disposal of consumer information into the information security program that the Safeguards Rule requires. (See [www.ftc.gov/privacy/privacyinitiatives/safeguards.html](http://www.ftc.gov/privacy/privacyinitiatives/safeguards.html).)

The Fair and Accurate Credit Transactions Act, which was enacted in 2003, directed the FTC, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Securities and Exchange Commission to adopt comparable and consistent rules regarding the disposal of sensitive consumer report information. The FTC’s Disposal Rule became effective June 1, 2005. It was published in the Federal Register on November 24, 2004 [69 Fed. Reg. 68,690], and is available at [ftc.gov/os/2004/11/041118disposalfrn.pdf](http://ftc.gov/os/2004/11/041118disposalfrn.pdf).

## In Case of a Security Breach

An “information security incident” is defined as the attempted or successful unauthorized acquisition, access, use, disclosure, modification or destruction of company information. The source of such incidents may be either internal or external. An information security incident will most often occur with personal information stored in an electronic format but also may involve unauthorized acquisition, access, use, disclosure or destruction of sensitive personal information stored in the paper media. Examples would include but not be limited to the following:

- Inappropriate access or acquisition of company information
- Attempts to gain unauthorized access to a computer system or its data
- Unauthorized use of a computer system for the processing or storage of data
- Unauthorized use of another associate’s account (e.g., using someone else’s ID or letting another person use yours)
- Unauthorized use of computer system privileges
- Lost or stolen computer or other electronic device or media (e.g., PDA, CDs, diskettes and backup computer tapes)
- Lost or stolen paper records

## Breach of Security Notification Laws

Many states have enacted laws that require companies that own or maintain sensitive personal information to provide notice to individuals who are affected by a “breach of security” event that involves the company. Not all information

security incidents will be considered a breach of security for purposes of sending breach notices. The definition for security breach varies from state to state, as does the definition of “personal information.” When combined, these two definitions set the standard for understanding when an information security incident triggers a legal requirement to send a breach-of-security notice to affected individuals.

## **Relationship to Other Laws**

Breach of security notification laws are separate from other state or federal laws regulating the privacy and/or security (safeguarding) of non-public personal financial or secured health information maintained by each company. The privacy and security laws generally affect information that companies collect, use or disclose that relates to customers or prospective customers. Breach-of-security notification laws generally apply to sensitive personal information that companies own or maintain for any individual (e.g., customers, prospective customers, agents, prospective agents, employees, prospective employees, Board of Directors or any other individual for whom companies store and/or maintain sensitive personal information).

NOTE: Information security incidents may require compliance action under existing privacy and/or security laws (e.g., mitigation requirements), as well as the breach of security notification laws.

## **Case Studies and Important References**

Case studies and important government and private-sector Internet references can be found on the NAILBA website on the Security reference page at <http://www.nailba.org/content/technology/security.cfm>.

## Appendix: Information Security Checklist

Completed	Security Action	Notes
<input type="checkbox"/>	Identify all classified information to be safeguarded.	See guidelines on page 4.
<input type="checkbox"/>	Designate business owners for all information assets.	See guidelines on page 5.
<input type="checkbox"/>	Safeguard policyholder files: shorten names, truncate account numbers and encrypt confidential information.	
<input type="checkbox"/>	Create and enact a new secure password policy.	See guidelines on page 6.
<input type="checkbox"/>	Secure all servers: <ul style="list-style-type: none"> <li>• Create and maintain firewalls.</li> <li>• House all Internet-facing servers in an isolated DMZ.</li> <li>• Set up anti-spam and anti-virus email filters.</li> <li>• Use a web-filtering solution to limit Internet access.</li> </ul>	See guidelines on page 7.
<input type="checkbox"/>	Secure all workstations and laptops: <ul style="list-style-type: none"> <li>• Advise all employees to lock workstations and log off all applications before leaving.</li> <li>• Password-secure all workstations/laptops.</li> <li>• Keep operating systems/applications patched/updated.</li> <li>• Configure personal firewall/intrusion detection systems.</li> <li>• Install an encryption system (disk/file level).</li> </ul>	See guidelines on page 8.
<input type="checkbox"/>	Perform data backups regularly.	
<input type="checkbox"/>	Enact a policy to safeguard laptops and their data.	See guidelines on page 8.
<input type="checkbox"/>	Safeguard wireless access to corporate networks.	
<input type="checkbox"/>	Secure and password-secure all PDAs/mobile phones.	See guidelines on page 8.
<input type="checkbox"/>	Disable USB/FireWire ports and encrypt portable storage devices.	
<input type="checkbox"/>	Securely store, encrypt and password-secure all backup tapes/media.	
<input type="checkbox"/>	Secure hard-copy confidential information in locked rooms/cabinets; shred outdated information.	See guidelines on page 9.
<input type="checkbox"/>	Establish strict guidelines for the employee handling of confidential documents.	
<input type="checkbox"/>	Keep all fax machines in a secure area.	
<input type="checkbox"/>	Take appropriate steps to destroy papers and electronic files/media containing consumer report information.	See guidelines on page 10.
<input type="checkbox"/>	Create an "Information Security Policy" by documenting all security practices and actions in writing.	