# Checklist for **Creating Plan**

The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operation, including three areas that are particularly important to information security: Employee Management and Training; Information Systems; and Detecting and Managing System Failures. Not each of these recommendations will apply to circumstances found in tax preparer offices, but they still provide the building blocks for the creation of a security plan and reinforce IRS recommendations that tax professionals establish strong security protocols. Depending on the nature of their business operations, firms should consider implementing the following practices:

## Employee Management and Training

| | Ongoir | Don | N/A |
|---|---|---|---|
| The success of your information security plan depends largely on the employees who implement it. Consider these steps: | ☐ | ☐ | ☐ |
| The success of your information security plan depends largely on the employees who implement it. Consider these steps: | ☐ | ☐ | ☐ |
| Check references or doing background checks before hiring employees who will have access to customer information. | ☐ | ☐ | ☐ |
| Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information. | ☐ | ☐ | ☐ |
| Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs. | ☐ | ☐ | ☐ |
| Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.) **(IRS suggestion: passwords should be a minimum of eight characters, the NIST standard. Prevent password sharing; ensure each employee with access to taxpayer accounts uses a unique password.)** | ☐ | ☐ | ☐ |
| Use password-activated screen savers to lock employee computers after a period of inactivity. | ☐ | ☐ | ☐ |
| Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device. | ☐ | ☐ | ☐ |
| Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including: | ☐ | ☐ | ☐ |
| • Locking rooms and file cabinets where records are kept; | ☐ | ☐ | ☐ |
| • Not sharing or openly posting employee passwords in work areas; | ☐ | ☐ | ☐ |
| • Encrypting sensitive customer information when it is transmitted electronically via public networks; | ☐ | ☐ | ☐ |
| • Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and | ☐ | ☐ | ☐ |
| • Reporting suspicious attempts to obtain customer information to designated personnel. | ☐ | ☐ | ☐ |

| | Ongoin | Done | N/A |
|---|---|---|---|
| Regularly remind all employees of your company's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms. | ☐ | ☐ | ☐ |
| Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions. | ☐ | ☐ | ☐ |
| Impose disciplinary measures for security policy violations. | ☐ | ☐ | ☐ |
| Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures. **(IRS Suggestion: Deactivate access prior to termination.)** | ☐ | ☐ | ☐ |
| (IRS Suggestion: Add labels to documents to signify importance, such as "Sensitive" or "For Official Business" to further secure paper documents.) | ☐ | ☐ | ☐ |

# Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some FTC suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal:

| | | | |
|---|---|---|---|
| Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example: | ☐ | ☐ | ☐ |
| • Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods. | ☐ | ☐ | ☐ |
| • When customer information is stored on a server or other computer, ensure the computer is accessible with a "strong" password and is kept in a physically secure area. **(IRS Suggestion: If using a cloud storage service, use a strong password, multi-factor authentication options and beware of thieves posing as providers.)** | ☐ | ☐ | ☐ |
| • Where possible, avoid storing sensitive customer data on a computer with an Internet connection. | ☐ | ☐ | ☐ |
| • Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area. | ☐ | ☐ | ☐ |
| • Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored. | ☐ | ☐ | ☐ |
| Take steps to ensure the secure transmission of customer information. For example: | ☐ | ☐ | ☐ |
| • When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit. **(IRS Suggestion: Transport Layer Security 1.3 is newer and more secure.)** | ☐ | ☐ | ☐ |
| • If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message. | ☐ | ☐ | ☐ |
| • If you must transmit sensitive data by email over the Internet, be sure to encrypt the data. **(IRS Suggestion: Rather than using email, transmit files via Secure File Transfer Protocol (SFTP), successor to File Transfer Protocol (FTP)).** | ☐ | ☐ | ☐ |

| | | | |
|---|---|---|---|
| Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule. For example: | ☐ | ☐ | ☐ |
| • Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group. | ☐ | ☐ | ☐ |
| • Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed. | ☐ | ☐ | ☐ |
| • Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information. | ☐ | ☐ | ☐ |

# Detecting and Managing System Failures

Effective security management requires your company to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:

| | | | |
|---|---|---|---|
| Monitor the websites of your software vendors and read relevant industry publications for news about emerging threats and available defenses. | ☐ | ☐ | ☐ |
| Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to: | ☐ | ☐ | ☐ |
| • check with software vendors regularly to get and install patches that resolve software vulnerabilities; | ☐ | ☐ | ☐ |
| • use anti-virus and anti-spyware software that updates automatically; | ☐ | ☐ | ☐ |
| • maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations; | ☐ | ☐ | ☐ |
| • regularly ensure that ports not used for your business are closed; and | ☐ | ☐ | ☐ |
| • promptly pass along information and instructions to employees regarding any new security risks or possible breaches. | ☐ | ☐ | ☐ |
| Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to: | ☐ | ☐ | ☐ |
| • keep logs of activity on your network and monitor them for signs of unauthorized access to customer information; | ☐ | ☐ | ☐ |
| • use an up-to-date intrusion detection system to alert you of attacks; | ☐ | ☐ | ☐ |
| • monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and | ☐ | ☐ | ☐ |
| • insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges. | ☐ | ☐ | ☐ |

| | | | |
|---|---|---|---|
| Take steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs: | ☐ | ☐ | ☐ |
| • take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet; | ☐ | ☐ | ☐ |
| • preserve and review files or programs that may reveal how the breach occurred; and if feasible and appropriate, bring in security professionals to help assess the breach as soon as possible. | ☐ | ☐ | ☐ |
| Consider notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example: | ☐ | ☐ | ☐ |
| • notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm; | ☐ | ☐ | ☐ |
| • notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm; | ☐ | ☐ | ☐ |
| • notify the credit bureaus and other businesses that may be affected by the breach. See Information Compromise and the Risk of Identity Theft: Guidance for Your Business; and | ☐ | ☐ | ☐ |
| • check to see if breach notification is required under applicable state law. | ☐ | ☐ | ☐ |
| • (IRS suggestions: Practitioners who experience a data loss should contact the IRS and the states. Also, consider having a technical support contract in place, so that hardware events can be fixed within a reasonable time and with minimal disruption to business availability.) | ☐ | ☐ | ☐ |