Safeguarding Taxpayer Data

WRITTEN INFORMATION SECURITY PLAN

PRESENTED BY:

INTEGRITY TECHNOLOGIES

PREPARED FOR:

ABC Company

po box 123
Anytown CA 00000
Phone: 555-555-1212

Glossary

Adware

Computer advertising software that may or may not monitor computer use to target ads.

Confidentiality

Restrictions placed on information access and disclosure, including means for protecting personal privacy and proprietary information.

Denial of Service

An attack that prevents or impairs the authorized use of networks, systems or applications by exhausting resources.

Encrypt

To convert plain text to unintelligible text using a cryptographic algorithm.

Information Security

The process that ensures the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

Intrusion Detection

The act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource.

Keylogging

The action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored. Often secretly downloaded by malware, keylogging enables the theft of usernames and passwords among other things.

Malware

Refers to malicious software (malware) programs designed to damage or perform other unwanted actions on a computer system. Examples of malware are viruses, worms, Trojan horses, and spyware.

Management Safeguards

The security safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security.

Multi-factor Authentication

A security system that requires returning users to enter more than just credentials (username and password) to access an account or device, such as two-factor or three-factor authentication. Example: e-Services is protected by IRS Secure Access, a two-factor authentication process that requires returning users to enter their credentials and a security code sent as text to a mobile phone. Tax professionals should always use the highest multifactor authentication available.

Operational Safeguards

Security for an information system that is primarily implemented and executed by people rather than by a system.

Phishing

An attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate.

Ransomware

A type of malicious software, or malware, designed to block access to a computer system until a ransom is paid. Ransomware is typically spread through phishing emails or by unknowingly visiting an infected website.

Risk

The likelihood that the unwanted impact of an incident will be realized.

Risk Assessment

The process of identifying risks and determining the probability of occurrence, the resulting impact and additional security controls that would mitigate this impact.

Risk Management

The process of managing risks through risk assessment, cost-benefit analysis; the selection, implementation, and assessment of security controls, and the formal authorization to operate the system. The process includes consideration of effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

Safeguard

Protective measures are prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Security Controls

Safeguards are designed to protect the confidentiality, integrity and availability of a system and its information.

Security Plan

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Spear Phishing

Phishing attempts directed at specific individuals or companies; attackers may gather personal information about their target to increase their probability of success. This technique is by far the most successful on the Internet today, accounting for 91% of attacks

Spyware

Software installed into an information system to gather information on individuals or organizations without their knowledge.

Social Engineering

The manipulation of people into performing actions such as deviating from standard security practices or divulging confidential information that give attackers access to systems or confidential information.

Technical Safeguards

Controls for a system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

Threat

Any circumstance or event with the potential to adversely impact operations, assets or individuals through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

Trojan Horse

A computer program used to attack a computer system by secretly allowing, among other things, unauthorized access or alteration of data or software.

Virus

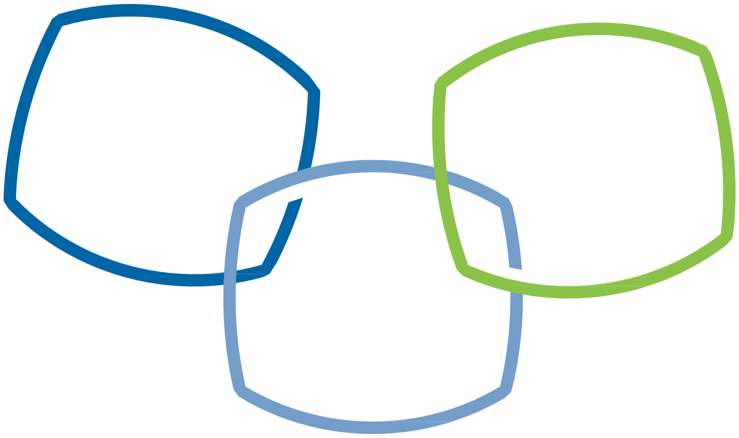
A computer program used to compromise a computer system by performing functions that may be destructive. A virus may alter other programs to include a copy of itself and execute when the host program or other executable component is executed.

Vulnerability

Weakness in a system through procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Worm

A computer program used to compromise a computer system by impacting performance. A worm can travel from computer to computer across network connections replicating itself.



Introduction - Safeguarding Taxpayer Data

Working Together to Combat Cybercrime in the Tax Industry

Addressing today's cyber threats requires a united effort. The Internal Revenue Service (IRS), in collaboration with state tax agencies and the tax industry, is committed to combating 21st-century identity theft. Through the formation of the Security Summit and the implementation of a series of safeguards, these partners have made significant progress. However, the work is far from over.

Data breaches targeting tax professionals are increasing. As the Security Summit strengthens protections, identity thieves are intensifying their efforts to obtain taxpayer data for filing fraudulent returns. Tax professionals, whether part of a large firm or operating independently, are now prime targets. As such, robust data security is essential for every tax practitioner and every Authorized IRS e-File Provider. All staff, including both professional and administrative personnel, must be educated on security threats and the measures needed to prevent them. Everyone has a role in safeguarding taxpayer information.

Protecting Taxpayer Data: A Legal Obligation

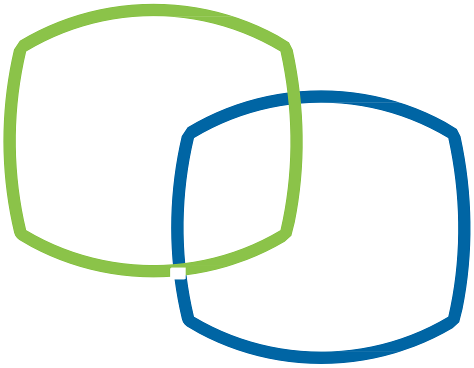
Federal law mandates the protection of taxpayer data. The Federal Trade Commission (FTC) is authorized to establish data safeguard regulations for various entities, including professional tax return preparers. Under the FTC Safeguards Rule, tax preparers are required to develop and implement written security plans to protect client information. For guidance, refer to IRS Publication 5708. Noncompliance may result in an FTC investigation. Additionally, online providers must adhere to the six security and privacy standards outlined in IRS Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns.

Protecting Taxpayer Data: A Smart Business Practice

Strong data security not only protects your clients, it also protects your business. A data breach can lead to reputational damage, client loss, and financial harm. Consider consulting cybersecurity professionals or speaking with your professional liability insurance provider about coverage for data breaches.

This guide is designed to help tax professionals:

- Understand and implement essential security practices
- Identify signs of data theft and know how to report incidents
- Respond to and recover from data breaches
- Comply with the FTC Safeguards Rule



Protect Your Clients; Protect Yourself

Take Basic Security Steps

Here are some basic security steps that tax professionals can take today to make their clients' data and their businesses safer:

- Learn to recognize phishing emails, especially those pretending to be from the IRS, e-Services, a tax software provider or cloud storage provider. Never open an embedded link or any attachment from a suspicious email.
- Create a data security plan using IRS **Publication 4557**, Safeguarding Taxpayer Data, and **Small Business Information Security – The Fundamentals,** by the National Institute of Standards and Technology.
- Review internal controls:
    - Install anti-malware/anti-virus security software on all devices (laptops, desktops, routers, tablets, and phones) and keep software set to automatically update, or have your IT provider manage security updates.
    - Use strong passwords of 12 or more characters, use different passwords for each account, use special and alphanumeric characters, use phrases, password protect wireless devices and consider a password manager program.
    - Implement **multi-factor authentication** for anyone accessing customer information on your system.
    - Encrypt all sensitive files/emails, especially those with the taxpayer's personally identifiable information (PII), and use strong password protections.
    - Back up sensitive data to a safe and secure external source not connected full-time to a network.
    - Make a final review of return information – especially direct deposit information - prior to e-filing.
    - Wipe clean or destroy old computer hard drives and printers that contain sensitive data to DoD standards.
    - Limit access to taxpayer data to individuals who need to know.
    - Check e-File Applications and PTIN accounts weekly for total returns filed using EFINs and PTINs; deactivate unused EFINs.
    - Withdraw from any outstanding authorizations (power of attorney/ tax information) for taxpayers who are no longer clients.
    - Implement audit trails (audit logs) that record all activities that occur. This includes who performed the activity, when it was performed, and what changes were made.

  - Implement a clean desk policy – sensitive data should never be left unattended.

- Report any data theft or data loss to the appropriate **IRS Stakeholder Liaison**.

- Stay connected to the IRS through subscriptions to **e-News for Tax Professionals, QuickAlerts** and **Social Media**.

- Educate clients about the availability of the Identity Protection PIN for taxpayers.

- Review the FTC's security tips at **Cybersecurity for Small Business** and **Protecting Personal Information: A Guide for Business**

Use Security Software

- A fundamental step to data security is the installation and use of security software on your computers. Here are the various types of security software you need and their purpose:

  - Anti-virus – prevents bad software, such as malware, from causing damage to a computer.

  - Zero-Trust – is a security model that requires verifying every user and device, every time, with no implicit trust until a security posture check has verified. **"Never trust, always verify."**

  - Firewall – blocks unwanted connections.

  - Drive Encryption – protects information from being read on computers, tablets, laptops, and smartphones if they are lost, stolen, or improperly discarded.

Windows and Mac operating systems include built-in security software and encryption capabilities. To ensure these features meet your organization's standards, consult with your IT provider and confirm compatibility with their hardware and encryption requirements. Additionally, an enterprise-grade antivirus solution should be installed, one that is centrally managed through a security portal. This solution should enforce policies that prevent users from disabling antivirus protection or the system firewall locally.

It's best practice to have your IT provider manage operating system and third-party security updates. This ensures updates are installed correctly and consistently. Additionally, your IT team will receive alerts if an update fails, helping to quickly address vulnerabilities before they can be exploited.

Alternatively, set security software to update automatically. This step is critical to ensuring the software has the latest protections against emerging threats. For additional safety, ensure that your internet browser (Chrome, Edge, Firefox, Safari, etc.) is set to update automatically so that it remains secure.
NOTE: You must check these periodically to ensure updates are being installed.

Create Strong Passwords

It is critical that all tax practitioners establish strong, unique passwords for all accounts, whether it's to access a device, tax software products, cloud storage, wireless networks, or encryption technology. Here's how to get started:

- Use a minimum of 12 characters; consider minimum of 16 characters for an administrator's password.
- Use a combination of letters, numbers, and symbols, i.e., ABC, 123, !@#.
- Avoid personal information or common passwords.
- Change default/temporary passwords that come with accounts or devices, including printers, routers, or smart devices.
- Do not reuse passwords, e.g., changing Bgood@IRS!17 to Bgood@IRS!18 is not good enough; use unique usernames and passwords for accounts and devices.
- Do not disclose your passwords to anyone for any reason; do not share passwords among employees. Each individual with access to client accounts should have a unique password. Use a password manager that's secured with MFA to track passwords, but protect it with a strong password.

Do not overlook a critical step to protecting accounts: **Multi-factor authentication**. This simple feature can protect your accounts even if your username and password are stolen. Tax software products for both taxpayers and tax professionals now offer multi-factor authentication.
Use the most secure option available, not only for your tax software, but other products such as email accounts and storage provider accounts. An example of multi-factor authentication: you must enter your credentials (username and password) plus a security code sent as a text to your mobile phone before you can access an account.

If hosting your own website, add some other form of multifactor authentication to further increase your login security.

Secure Wireless Networks

Failing to protect your wireless network makes the network or data vulnerable to attack or interception by cybercriminals. Thieves could be stealing your data without your knowledge. If you use wireless, you can take these protective steps by setting up your router or review your router's manual to make changes. Here are basic steps:

- Change the default administrative password of your wireless router; use a strong, unique password.

- Reduce the power (wireless range) so you are not broadcasting further than you need. Log into your router to WLAN settings, advanced settings and look for Transmit (TX) power. The lower the number the lower the power.
- Change the name of your router (Service Set Identifier - SSID) to something that is not personally identifying (i.e., BobsTaxService), and disable the SSID broadcast so that it cannot be seen by those who have no need to use your network.
- Use Wi-Fi Protected Access 3 (WPA-3).
- Do not use Wired-Equivalent Privacy (WEP) to connect your computers to the router; **WEP is not considered secure**.
- Never use a public Wi-Fi (for example, at a coffee café or airport) to access business email or sensitive documents. These networks are often unsecured and can expose your data to cyber threats. Instead, discuss secure alternatives with your IT provider, such as using a Virtual Private Network (VPN) or implementing a **Zero Trust Network Access (ZTNA)** solution to ensure safe remote access.

Use of multi-factor authentication (discussed earlier) and a secure Virtual Private Network (VPN) or Zero Trust Network Access (ZTNA) should be minimum standards for remote access to the firm's office network. A VPN provides a secure, encrypted tunnel to transmit data between a teleworking employee and the company network. Search for "Best VPNs" to find a legitimate vendor. Some firms issue laptops to remote-work employees to better secure the IT environment.

Protect Stored Client Data

Cybercriminals work hard through various tactics to penetrate your network or trick you into disclosing passwords. They may steal the data, hold the data for ransom, or use your computers to complete and file fraudulent tax returns. Here are a few basic steps to protect client data stored on your systems:

- Back up encrypted client data to secure external drives (e.g., encrypted USB hard drives or flash drives) and to cloud storage that supports versioning and prevents deletion from the source system—key defenses against ransomware. Store external drives securely, and always encrypt data before uploading to the cloud. Use drive encryption to lock files and all devices; encrypted files require a password to open.
- Never connect USB or external drives containing client data to any computer that hasn't been secured by your IT provider or internal IT team.
- Never access client data on a system that has not been secured by your IT provider or internal IT team.
- Avoid installing unnecessary software or applications to the business network; download software or applications only from official sites, or refer to your internal handbook regarding supported software for your organization.

- Perform an inventory of devices where client tax data is stored, i.e., laptops, smartphones, tablets, external hard drives, etc.; inventory software used to process or send tax data, i.e., operating systems, browsers, applications, tax software, web sites, etc.
- Limit or disable internet access capabilities for devices that have stored taxpayer data or access to PII data.
- Delete all information from devices using DoD standards, such as: hard drives, USBs (flash drives), printers, tablets, or phones before disposing of devices; some security software includes a “shredder” that electronically destroys stored files.
- Use DoD standards to destroy: hard drives, tapes, USBs, CDs, tablets, or phones; shred all documents containing taxpayer information before throwing away or recycling.

Be on Guard

Spot Data Theft

You or your firm may be a victim and not even know it. Here are some common clues to data theft:

- Client e-filed tax returns begin to reject because returns with their Social Security numbers were already filed.
- Clients who haven't filed tax returns begin to receive authentication letters (5071C, 4883C, 5747C) from the IRS.
- Clients who haven't filed tax returns receive refunds.
- Clients receive tax transcripts they did not request.
- Clients who created an IRS online services account receive an IRS notice that their account was accessed or IRS emails stating their account has been disabled; or, clients receive an IRS notice that an IRS online account was created in their names.
- The number of returns filed with tax practitioner's Electronic Filing Identification Number (EFIN or Preparer Tax Identification Number (PTIN)) exceeds number of returns you actually filed.
- Tax professionals or clients responding to emails that the practitioner did not send.
- Network computers running slower than normal or computers turning themselves on.
- Computer cursors moving or changing numbers without touching the keyboard.
- Network computers locking out tax practitioners.

Monitor EFIN/PTINs

You can obtain a weekly report of the number of tax returns filed with your Electronic Filing Identification Number or your Preparer Tax Identification Number. Only those preparers who are attorneys, CPAs, enrolled agents or Annual Filing Season Program participants and who file 50 or more returns may obtain PTIN information. Weekly checks will help flag any abuses. Here's how:

For EFIN totals:

- Access your e-Services account and your EFIN application;
- Select “EFIN Status” from the application;
- Contact the IRS e-help Desk if the return totals exceed the number of returns you filed.

For PTIN totals:

- Access your online PTIN account;
- Select “View Returns Filed Per PTIN;”
- Complete Form 14157, Complaint: Tax Return Preparer, to report excessive use or misuse of PTIN.

If you have a Centralized Authorization File (CAF) number, make sure you keep your authorizations up to date. Remove authorizations for taxpayers who are no longer your clients. (See “Withdrawal of Representation” in Publication 947, Practice Before the IRS and Power of Attorney.)

Recognize Phishing Scams

All employees in your office must be educated about the dangers of phishing scams. These scams can result in cybercriminals taking over your computer or accounts to steal client data.

- Cyber awareness training is a mandatory requirement for maintaining compliance with most cyber insurance policies. At a minimum, this training should be conducted annually, though you should confirm specific requirements with your insurance provider. It’s essential to document participation in a way that clearly demonstrates due diligence and helps protect against claims of negligence.
- A common way cybercriminals steal data is by using phishing scams. An even more successful tactic is called spear phishing, where the thief specifically targets you or your firm, perhaps seeing your email address from the office website.
- The thief may pose as your tax software provider, your data storage provider, the IRS, or even a prospective client. The thief may pose as your bank or as a professional colleague whose email was compromised.
- Thieves may hijack your email account to send spam emails under your name, tricking colleagues and clients into disclosing information. This is known as a Breach Email Compromise (BEC) and was the largest form of attacks in 2024.
- It is common for phishing or spear phishing emails to have an urgent subject line. Example: Update Your Account Now. The objective is to entice you to open a link or an attachment.
    - **Link:** The link may take you to a fake web page designed to look like a familiar website. Example: IRS e-Services. Again, there will be a call to action, such as “Click here NOW.” You may be asked

to enter your username and password for an account, but you are actually disclosing your credentials to thieves.

  - **Attachment:** The attachment may contain computer code called malware that can infect your computer and network systems. A common malware is keystroke tracking, which allows the criminal to see the words you type on your device, eventually disclosing your username and password to various accounts. In turn, this gives them access to your tax software provider, bank or encrypted client files..

- A legitimate business should never email and request personal or sensitive information to be sent to them via email, unless through a secured email service.

Guard Against Phishing Emails

Educated employees are the key to avoiding phishing scams, but these simple steps can also help protect against stolen data:

- Use separate personal and business email accounts; protect email accounts with strong passwords and two-factor authentication.
- Use security software to help protect systems from malware and a security layer that scans emails for phishing and viruses before they hit your inbox.
- Never open or download attachments from unknown senders, including potential clients; make contact first by phone, for example.
- Send only password-protected and encrypted documents if you must share files with clients via email. One-time access links with encrypted emails, along with an access self destruct is ideal.
- Do not respond to suspicious or unknown emails; if IRS-related, forward to your IT Partner or **phishing@irs.gov**.

Be Safe on the Internet

Data security takes an ongoing awareness of the threats posed by a variety of sources, including browsing the Internet. Here are some general steps for staying safe while using the Internet or protecting your website.

- Keep your web browser software up to date so it has the latest security features.
- Scan files using your security software before downloading to your computer.
- Look for the “S” in “HTTPS” connections for Uniform Resource Locator (URL) web addresses. The “S” stands for secure, e.g., https://www.irs.gov.
  - This doesn’t mean the website itself is secure; it simply means that the data sent over the connection is encrypted and can’t be easily intercepted on a public network.
- Avoid accessing business emails or information from public wi-fi connections.
- Disable stored password feature offered by some operating systems.
- Do not download files, software, or applications from unknown websites. Refer to your handbook or IT provider to reference approved applications
- Note if your browser homepage changes; it could be a sign of malware or an intrusion. Review your last downloads and browser settings, check to see if you have anything new in your toolbar.

Report and Respond

Report Data Loss to IRS/States

Tax practitioners should report data losses or thefts immediately to the IRS so that appropriate precautions can be made to protect clients from fraudulent returns being filed in their names. Here's how to report data thefts to the IRS:

- Contact the IRS and law enforcement:
  - **Internal Revenue Service**, report client data theft to your local stakeholder liaison.
  - **Federal Bureau of Investigation**, your local office (if directed by IRS).
  - Local police – To file a police report on the data breach.
- Contact states in which you prepare state returns:
  - Visit the **Federation of Tax Administrators** "Report a Data Breach" to find state contact information.
- Contact experts:
  - Security expert – to determine the cause and scope of the breach, to stop the breach, and to prevent further breaches from occurring.
  - Insurance company – to report the breach and to check if your insurance policy covers data breach mitigation expenses.

For a complete checklist, see **Data Theft Information for Tax Professionals.**

If you are a victim of a ransomware attack, please contact the FBI and Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) in addition to the IRS.

Respond and Recover from a Data Loss

The Federal Trade Commission offers assistance to businesses who were victimized by data thefts and provides templates for letters that, for example, notify clients that a data loss has occurred. Here are some basic suggestions on how to recover from a data theft:

- Update your IRS Stakeholder Liaison with developments; IRS telephone assistors cannot accept third-party reports of identity theft.
- Review FTC's Data Breach Response: A Guide for Business for helpful guidance in notifying clients and tips for responding and recovering.
- Determine how the intrusion or theft occurred and make any required fixes before resuming tax preparation activities and being issued a new Electronic Filing Identification Number (EFIN).
- Develop a continuity plan.
- Make full backups of all business data and files. If you weren't doing:
    - A routine backup means you will have a copy of your data. A data loss or ransomware attack (as well as a hurricane or flood) will not destroy all your files.
    - Encrypt backed-up files.
    - Consider a nightly backup schedule.
    - Backup files after completing a routine system scan.
    - Use an external hard drive or cloud storage; encrypt files prior to uploading data.

Consult with your professional insurance provider about data theft protection.

- Insurance firms can help preparers recover from a theft.
- Insurance firms may help provide security experts to analyze protections or detect intrusions.

Comply with the FTC Safeguards Rule

Understand the FTC Safeguards Rule

Under the Safeguards Rule, financial institutions must protect the consumer information they collect. The Gramm-Leach-Bliley (GLB) Act requires companies defined under the law as “financial institutions” to ensure the security and confidentiality of this type of information. The “financial institutions” definition includes professional tax preparers.

As part of its implementation of the GLB Act, the **Federal Trade Commission** issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. The **Safeguards Rule** requires companies to develop a written information security plan that describes their program to protect customer information. See **Publication 5708** for information on creating a written information security plan.

Comply with the FTC Safeguards Rule

According to the FTC, the required information security plan must be appropriate to the company’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program;
- Implement Multi-factor Authentication. Implement for anyone accessing customer information on your system. The FTC Safeguards Rule requires at least two of the following authentication factors: a knowledge factor (for example a password), a possession factor (for example, a token), and an inherence factor (for example biometric information). This is required for all companies regardless of size.
- Identify and assess the risks to customer information in each relevant area of the company’s operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- Design and implement a safeguards program, and regularly monitor and test it; select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and evaluate and adjust the program in light of relevant circumstances, including changes in the firm’s business or operations, or the results of security testing and monitoring.
- Provide security awareness training and schedule regular refreshers.

ABC Company - CyberSecurity Attestation

Question	Answer
Check references or do background checks before hiring employees who will have access to customer information.	Yes
Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.	Yes
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.	Yes
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 12 characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.) IRS suggestion: passwords should be a minimum of 12 characters, according to the NIST standard. Prevent password sharing; ensure each employee with access to taxpayer accounts uses a unique password.	Yes
Require multi-factor authentication for anyone accessing customer information on your system.	Yes
Use password-activated screen savers to lock employee computers after a period of inactivity.	Yes
Develop policies for appropriate use and protection of laptops, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. All devices that store or have access to customer data should have full disk encryption	Yes
Locking rooms and file cabinets where records are kept:	Yes
Not sharing or posting any passwords in work areas.	Yes
Encrypting sensitive customer information when it's transmitted electronically via public networks, and reporting suspicious attempts to obtain customer information to designated personnel, ie, Phishing.	Yes
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.	Yes
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 company-approved protections against malware, full-disk encryption, follow the password policy on all user accounts, and lock-screen timeouts	Yes
Implement mandatory Cyber Awareness Training, with full logs kept of when the training was given, and employee acknowledgement of the training.	Yes

ABC Company - CyberSecurity Attestation

Question	Answer
Prevent terminated employees from accessing customer information by immediately deactivating their user names and taking other appropriate measures. Create a policy to follow proper steps after an employee leaves to prevent any network or data access.	Yes
Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.	Yes
Store records in a room or cabinet that is locked when unattended.	Yes
When customer information is stored on a server or other computer, ensure that the computer is accessible only 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.	Yes
Where possible, avoid storing sensitive customer data on a computer with an Internet connection that's used for browsing.	Yes
Maintain secure backup records and keep archived data secure by storing it offline and in a physically secure area.	Yes
Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.	Yes
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 1.2 or 1.3 is newer and more secure	Yes
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	Yes
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 Secured Portal that requires authentication to access.	Yes
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.	Yes
Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.	Yes
Destroy or erase data to DoD standards when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.	Yes
Monitor the websites of your software vendors and read relevant industry publications for news about emerging threats and available defenses. IT providers can help you with this.	Yes

ABC Company - CyberSecurity Attestation

Question	Answer
Check with software vendors regularly to get and install patches that resolve software vulnerabilities. **Best Practice:** Ask your IT partner to handle your Windows, Mac, and 3rd party updates	Yes
Use an anti-virus that updates automatically. **Best Practice:** An enterprise-level anti-virus should be installed that can be managed through a security portal, and a policy should be in place to not allow local disabling of the antivirus or firewall.	Yes
Maintain and monitor up-to-date firewalls. **Best Practice:** Use a hardware firewall that alerts you or your IT partner when updates are available. Hackers target router and firewall vulnerabilities and tunnel their way straight into your network.	Yes
Regularly ensure that ports not used for your business are closed via network assessment. **Best Practice:** Perform a 3rd party network assessment for internal and external vulnerabilities.	Yes
Keep activity logs on your network and monitor them for signs of unauthorized access to customer information.	Yes
Use an up-to-date intrusion detection system to alert you of attacks.	Yes
Monitor both inbound and outbound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user. **Best Practice:** Use a 3rd party system for this monitoring, ask your IT provider to help you.	Yes
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. Important: If ransomware is a possibility, immediately shut down all systems on the network to prevent the spread	Yes
Notify your IT provider to start your Incident Response Plan; this can significantly reduce the blast radius of the attack. Notify your Cyber Insurance carrier if applicable; there is a specific order to handle the order of notifications, and the carrier will walk you through the correct steps. 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.	Yes
IRS suggestions: Practitioners who experience a data loss should contact the IRS and the state. 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.	Yes

ABC Company - CyberSecurity Attestation

Organization Security Officer: John Doe
Date reviewed and completed: 2025-09-21 01:42

I attest that the information provided in this form is complete and accurate to the best of my knowledge as a security officer.

John Doe

Signature