Checklist for Safeguarding Taxpayer Data

WISP in Practice: Protect Your Clients & Your License

Course Material Export – Generated for IRS Continuing Education Review

1.1 - What is a WISP (Written Information Security Plan) ?

Lesson at a Glance:

[Image: Written Information Security Plan]

A **Written Information Security Plan (WISP)** is a formal, documented policy that describes how your tax practice collects, stores, protects, and disposes of sensitive taxpayer data.

It is not a software product, a checklist you complete once, or a generic template you download and file away.

A WISP is a **living document** — specific to your firm, reviewed at least annually, and known by everyone in your office who touches client data.

The **IRS Security Summit**, the **FTC Safeguards Rule**, and the **Gramm-Leach-Bliley Act** all point to the same core requirement: if you handle nonpublic personal financial information, you must have a written plan to protect it.

Defining the WISP

Defining the WISP

The term **Written Information Security Plan (WISP)** comes directly from the FTC Safeguards Rule (16 C.F.R. Part 314), which was strengthened through regulatory updates that became effective in 2023.

For tax professionals, the IRS has aligned its guidance — primarily through **IRS Publication 4557** and annual **Security Summit** materials — with the FTC framework.

Every WISP must answer six fundamental questions about how your practice protects taxpayer information.

What Data?

What taxpayer information do we collect, process, and store?

Where Is It?

Computers, cloud storage, paper files, backup drives, and other locations.

Who Has Access?

Employees, contractors, seasonal staff, and remote users.

How Protected?

Passwords, MFA, encryption, physical security, and other safeguards.

What If Something Goes Wrong?

Incident response procedures, breach reporting, and recovery steps.

How Do We Stay Current?

Annual reviews, updates, training, and continuous improvement.

The Three Categories of Protected Data

[Image: WISP-3-scaled.webp]

Your WISP must address protections for all three forms of taxpayer data your practice handles:

Data Type	Examples	Risk if Exposed
Electronic data	Tax software files, PDFs, emails, cloud storage, scanned documents	Identity theft, fraudulent returns, refund theft
Physical data	Paper returns, intake forms, prior-year documents, printed 1099s	Dumpster-diving theft, office burglary
Verbal/transmitted data	Phone calls with clients, fax transmissions, information shared with IRS	Interception, impersonation fraud

What a WISP Is NOT

Common WISP Misunderstandings

One of the most common mistakes among small tax practices is assuming that a security tool or good habit automatically equals a Written Information Security Plan.

Antivirus Software

Installing antivirus software is a safeguard — not a Written Information Security Plan.

Secure Tax Software

Using a reputable tax software platform does not satisfy the requirement to maintain a written security program.

Strong Passwords

A strong password policy helps protect data, but it must be documented as part of the firm's written security procedures.

Downloaded Template

Downloading the IRS WISP template and never customizing it does not create a compliant WISP.

Locked Filing Cabinet

Physical security is important, but a locked cabinet alone does not explain who has access, how records are handled, or what happens during a breach.

What a WISP Really is

What a WISP Really Is

A WISP is not a product, software package, password, or filing cabinet.

A WISP is the **written documentation** that explains how your firm protects taxpayer information.

What Safeguards?

The security controls your practice uses to protect client data.

Why Use Them?

The risks those safeguards address and why they are necessary.

Who Is Responsible?

The individuals responsible for maintaining and enforcing the program.

What Happens Next?

How the firm responds when a breach, incident, or security event occurs.

The IRS template is a starting point — not a finished plan.

IRS Publication 5708

The Security Summit's downloadable **WISP template** is an excellent foundation, but it must be customized with the specifics of your practice.

- Your software vendors
- Your employee and contractor roles
- Your physical office layout

- Your actual security procedures

A template with blanks left unfilled does not constitute a compliant WISP.

The "Written" Requirement

The word **"written"** is intentional and legally significant. Oral policies, habits, and informal understandings do not meet the standard.

Your plan must exist as a document — electronic or paper — that can be produced, dated, signed, and reviewed.

- Produced on request
- Dated and version controlled
- Signed or approved by the practice
- Reviewed and updated regularly

In the event of an IRS examination or FTC enforcement action, you must be able to produce the actual WISP document — not simply describe your security practices from memory.

[Image: WISP Best Practice]

Best Practice

Store your WISP in at least two locations — one electronic and one printed copy.

- Electronic copy should be encrypted and backed up.
- Maintain a printed copy in a secure but accessible location.
- Date every version of the WISP.
- Sign each revision to create a clear audit trail.

Maintaining multiple copies and documenting every update demonstrates that your WISP is an active compliance program rather than a forgotten file.

Scenario — The "We Do All That Already" Preparer

Scenario

Prencess runs a solo tax practice from a home office. She uses reputable tax software, has antivirus installed, shreds old documents, and uses a strong password on her computer.

She has never written any of these procedures down in a formal document.

Analysis

Prencess has good security practices — but she does **not** have a WISP.

The FTC Safeguards Rule requires a **written** information security program. Security measures that are not documented may be difficult to demonstrate during a compliance review or after a data breach.

If a Breach Occurred

If Prencess's laptop were stolen and taxpayer information was compromised, she would have:

- No documented incident response procedure
- No designated security coordinator or breach contact
- No written evidence of a security program
- No documented proof that security procedures were being followed

The Solution

Prencess does not need to purchase additional software or replace her current security practices. She simply needs to:

- Document the safeguards she already uses
- Convert those safeguards into a written policy
- Add a formal incident response plan
- Designate a security coordinator
- Review and update the WISP annually

The security program already exists in practice. The missing requirement is putting it in writing and maintaining it as a living document.

1.2 - IRS Requirements: Who Must Have a WISP

[Image: Who-Must-Have-a-WISP.webp]

Lesson at a Glance

Every tax professional who is in the business of preparing or assisting in the preparation of federal tax returns is required to have a Written Information Security Plan. The obligation flows from the FTC Safeguards Rule under the Gramm-Leach-Bliley Act and is reinforced by IRS guidance. There is **no size exemption** — a solo preparer working from a spare bedroom faces the same legal obligation as a 50-person firm. The IRS has also made clear through its Security Summit communications that failure to maintain a WISP is a violation of a preparer's professional obligations and can factor into disciplinary proceedings under Circular 230.

Learning Objectives

After completing this lesson you will be able to:

- Identify which tax professionals are legally required to maintain a WISP.
- Explain the regulatory chain from GLBA to FTC Safeguards Rule to IRS guidance.
- Understand that firm size does not affect the requirement — only the complexity of the plan.
- Recognize the consequences of non-compliance under Circular 230 and the FTC Safeguards Rule.

The Legal Chain of Requirement

The WISP requirement for tax preparers does not come from a single law — it flows through a chain of interconnected regulations:

Law / Rule	What It Requires	Who Enforces It
Gramm-Leach-Bliley Act (GLBA)	Financial institutions — including tax preparers — must protect customers' nonpublic personal information	FTC
FTC Safeguards Rule (16 C.F.R. Part 314)	Written information security program required; updated rules effective 2023 added specific technical safeguards	FTC
IRS Publication 4557	Practical guidance for tax preparers implementing data security; explicitly references the WISP requirement	IRS (guidance)
Treasury Circular 230	Practice standards for tax professionals; incompetence or disreputable conduct includes failure to safeguard client data	IRS Office of Professional Responsibility
IRC §7216	Prohibits unauthorized disclosure or use of tax return information	DOJ / IRS

Who Is Covered

The FTC defines "financial institution" broadly for purposes of the Safeguards Rule. Tax preparation businesses — including sole proprietors — fall within this definition because they regularly receive nonpublic personal financial information from consumers in connection with a financial service. Covered preparers include:

- Enrolled Agents (EAs)
- Certified Public Accountants (CPAs) preparing returns
- Attorneys preparing returns
- Annual Filing Season Program (AFSP) participants

- Unenrolled preparers (PTIN holders) who prepare returns for compensation
- Bookkeepers and accounting staff who access and transmit taxpayer data on behalf of a preparer

[Image: part-time-job.webp]

Part-time and seasonal preparers are not exempt. If you prepare returns for compensation during tax season only, you are still operating a tax preparation business and must maintain a WISP for the period during which you handle taxpayer data. The plan does not need to be elaborate — but it must exist and be in writing

Part-time and seasonal preparers are not exempt.

Firm Size and Plan Complexity

The FTC Safeguards Rule acknowledges that a one-person operation should not be expected to implement the same infrastructure as a national firm. The rule uses a "size and complexity" standard — meaning your WISP must be appropriate to:

- The size and scope of your business
- The nature and sensitivity of the data you handle
- The cost and feasibility of available safeguards

In practice, a solo preparer's WISP will be shorter and simpler than a multi-location firm's. But "simpler" does not mean absent. A one-page WISP that genuinely addresses all required elements is fully compliant. A 40-page document that was never customized is not.

Consequences of Non-Compliance

Preparers who do not maintain a WISP face risk on multiple fronts:

- **FTC enforcement:** The FTC has authority to pursue civil penalties against businesses that violate the Safeguards Rule. Penalties can reach into the tens of thousands of dollars per violation per day.
- **IRS disciplinary action:** Under Circular 230, the IRS Office of Professional Responsibility (OPR) can censure, suspend, or disbar a practitioner for conduct that brings discredit to the tax profession — which includes failing to protect client data.
- **State-level consequences:** Many states have their own data security laws with independent penalties. A breach without a documented response plan can trigger state attorney general investigations.

- **Civil liability:** Clients whose data is compromised as a result of a preparer's failure to maintain reasonable safeguards may have civil claims against the preparer.
- **Reputational damage:** In a referral-driven business like tax preparation, a publicized breach can permanently damage client relationships.

Scenario — The Seasonal Preparer

[Image: TheSeasonalTaxPreparer.webp]

Macy prepares roughly 80 returns each tax season from January through April. She works from home, uses Drake tax software, and emails PDFs to clients. She has never created a WISP because he assumed the requirement only applies to "real" tax offices.

Analysis: Macy is wrong. She receives Social Security numbers, W-2s, bank account information, and health insurance data from 80 households. She is a tax preparation business under the FTC Safeguards Rule regardless of the season or volume. She needs a WISP. For someone in his situation, a well-completed two- to three-page plan addressing his home office setup, her software, how she transmits documents to clients, and what he would do in a breach is sufficient — and achievable in an afternoon using the IRS template as a guide.

Practitioner Tips

- **Create your WISP before the filing season begins** — not after a breach has already occurred. Regulators look at whether safeguards were proactively in place, not whether you scrambled to document them after an incident.
- **Keep a signed, dated copy.** Your signature and the date signal that you reviewed and adopted the plan. This matters in any enforcement or liability proceeding.
- **Your WISP should name a person.** Every compliant WISP designates a specific individual as the Information Security Coordinator (or equivalent). For solo preparers, that person is you.

1.3 - Real-World Breach Examples

[Image: Dat-Breaches-Targeting-tp.webp]

Lesson at a Glance

Data breaches targeting tax preparers are not rare events that happen to large corporations — they happen to small and solo practices every tax season. The IRS processes thousands of identity theft-related return fraud cases annually, and a significant

portion traces back to compromised tax preparer systems. This lesson examines common attack vectors that hit tax offices, the real-world consequences for both the preparer and their clients, and the single most consistent finding in post-breach investigations: **there was no written security plan, or the plan that existed was never tested or followed.**

Learning Objectives

After completing this lesson you will be able to:

- Identify the most common methods attackers use to breach tax preparer systems.
- Describe the consequences a breach has on clients, the preparer, and the preparer's license.
- Explain why small practices are frequently targeted rather than protected by their size.
- Connect the presence of a WISP to reduced breach likelihood and reduced liability after a breach.

How Tax Preparer Breaches Happen

Tax preparers are targeted for a specific reason: they are a one-stop source for everything an identity thief needs. A single client file contains a Social Security number, date of birth, address, employer, bank routing and account numbers, and often prior-year return data. The most common attack methods include:

1. Phishing Emails

A preparer receives an email that appears to come from their tax software provider, the IRS e-Services portal, or a payroll company. The email contains a link to a fake login page that captures the preparer's username and password. With those credentials, the attacker accesses the preparer's software account and extracts client data — or files fraudulent returns directly.

2. Remote Access Takeover

Many small offices use remote desktop tools so preparers can work from home or so clients can share their screens. Attackers scan for open remote access ports and use brute-force techniques or stolen credentials to gain access. Once inside, they have full access to all files on the network.

3. Ransomware

An employee opens an attachment or clicks a malicious link, and ransomware encrypts every file on the network. The attacker demands payment to restore access. Even if the preparer pays, there is no guarantee the data wasn't also copied and sold before encryption. Tax season ransomware attacks are timed to maximize pressure — attackers know preparers cannot afford downtime in February or March.

4. Physical Theft

A laptop left in a car, an unshredded client folder in a recycling bin, or an unlocked filing cabinet in an office that shares space with other businesses. Physical data breaches are less dramatic but equally damaging.

5. Insider Threat

A seasonal employee, a contractor, or a former staff member retains access to client data after their engagement ends. Without an access control policy — a core WISP component — departing employees often retain credentials and file access long after they should have been revoked.

How Tax Preparer Breaches Happen

Consequence	Details
IRS investigation	The IRS Stakeholder Liaison and Criminal Investigation division will contact the preparer. The preparer may be required to notify all affected clients and the IRS.
EFIN suspension	The IRS may suspend the preparer's Electronic Filing Identification Number (EFIN) while the investigation is ongoing — effectively shutting down the practice during filing season.
Circular 230 disciplinary action	The IRS Office of Professional Responsibility may open a proceeding that results in censure, suspension, or disbarment from practice before the IRS.
FTC enforcement	If the breach results from failure to maintain a Safeguards Rule-compliant security program, the FTC may pursue civil penalties.
State licensing action	State CPA boards and EA licensing bodies may take independent action based on the breach and the preparer's failure to have documented safeguards.
Civil lawsuits	Clients who suffer financial harm — fraudulent returns filed in their name, identity theft, credit damage — may pursue the preparer directly in civil court.

EFIN suspension during filing season is a business-ending event for many small practices.

[Image: block-brick-fire.svg]

Even a temporary suspension while the IRS investigates can result in clients leaving, deadlines being missed, and relationships being permanently damaged. The cost of building and maintaining a WISP is measured in hours. The cost of a breach without one is measured in years.

Consequences for Clients

- **When a tax preparer is breached, every client in the affected system is a potential victim:**
- Fraudulent federal and state returns filed in their name, stealing their refund
- New credit accounts opened using their Social Security number and personal data
- IRS notices demanding repayment of refunds they never received
- Months or years of identity theft recovery — filing Form 14039, requesting IP PINs, disputing credit accounts
- Emotional distress and loss of trust in the preparer

Scenario 1 — The Phishing Click

[Image: phishing.webp]

Linda, a solo EA, receives an email that looks exactly like a message from her tax software vendor asking her to verify her e-Services login. She clicks the link and enters her credentials. Within 48 hours, fraudulent returns are filed for 23 of her clients with refunds directed to prepaid debit cards.

Result: Linda had no WISP, no phishing awareness training documented, and no multi-factor authentication on her software accounts. The IRS suspends her EFIN. She must notify all 23 affected clients. Two clients file civil complaints. The IRS OPR opens a Circular 230 investigation. A simple multi-factor authentication requirement — a one-paragraph policy in a WISP — would have prevented the breach entirely.

Scenario 2 — The Unlocked Laptop

[Image: phishing.webp]

Kerry, who runs a two-preparer office, has a staff member whose laptop is stolen from her car in February. The laptop contained client files for the current and prior two tax years — approximately 400 client records. The laptop was not encrypted.

Result: Because there was no encryption policy (and therefore no encryption), all 400 client records are presumed compromised. Kerry must notify all 400 clients, report to the IRS, and file a report with the FTC. His state has a data breach notification law that triggers mandatory notification to the state attorney general within 30 days. An encryption requirement — another standard WISP element — would have meant the stolen laptop contained only unreadable data.

The WISP Connection

Post-breach investigations consistently show that the single most common factor in preventable tax preparer breaches is the absence of documented, implemented security policies. A WISP does not guarantee you will never be attacked. But it dramatically reduces risk by requiring you to actively identify vulnerabilities, implement controls, and train your staff — and it reduces your liability after a breach by demonstrating that you exercised reasonable care.

2.1 The 5 Core Elements

[Image: core-Wisp-element.webp]

The 5 Core Elements of a WISP & Conducting Your Risk Assessment

A compliant WISP is built on five core elements defined by the FTC Safeguards Rule and aligned with IRS guidance: a designated Information Security Coordinator, a data inventory and risk assessment, written safeguards for each identified risk, a vendor oversight provision, and an incident response and annual review plan. Of these five, the **risk assessment** is the foundation — you cannot write safeguards for risks you have not identified, and you cannot identify risks you have not inventoried. This lesson walks through all five elements in detail and then guides you through the step-by-step risk assessment process so that by the end, you have both the framework and the diagnostic tool needed to build a WISP that is specific to your practice rather than a generic document that satisfies no one.

This lesson walks through each element in detail so you understand not just what to include — but **why each element exists** and what it looks like in a real tax practice of any size.

Learning Objectives

After completing this lesson you will be able to:

- Name and explain each of the five core elements required in a compliant WISP.
- Describe what each element looks like in a small or solo tax practice.
- Complete a data inventory covering all three forms of client data in your practice.
- Identify and categorize threats — external, internal, and accidental.
- Use a likelihood-and-impact framework to prioritize risks and connect them to specific safeguards.
- Document your risk assessment in a format that satisfies the FTC Safeguards Rule.

Part 1 — The Five Core Elements

The FTC Safeguards Rule does not prescribe a specific format or length for your WISP — it prescribes outcomes. The five elements below represent the minimum components needed to achieve those outcomes. A plan that addresses all five is compliant regardless of whether it is two pages or twenty.

Element 1 — Designated Information Security Coordinator

Your WISP must name a specific individual responsible for implementing and overseeing the security program. The FTC calls this person the "Qualified Individual." The IRS uses the term "Information Security Coordinator." The title does not matter — what matters is that one named person is clearly accountable. For a solo preparer, this is you. For a multi-person office, it should be the owner or a designated senior staff member with the authority to enforce policies and act as the primary contact in a breach.

Sample language: "The Information Security Coordinator for [Firm Name] is [Full Name], [Title]. This individual is responsible for implementing, maintaining, and annually reviewing this Written Information Security Plan."

[Image: tc.webp]

The 2023 FTC Safeguards Rule update added a new obligation: the coordinator must report regularly to the firm's governing authority — for a small practice, the owner — on the status of the security program. Even if you are both the owner and the coordinator, add a dated annual entry to Section 8 of your WISP confirming you reviewed the plan and noting any changes made. This creates the audit trail the rule requires.

Element 2 — Data Inventory and Risk Assessment

You cannot protect what you have not identified. Your WISP must document what client data you collect, where it is stored, who has access to it, and what the risks are if it is compromised. This is the foundation on which every other element rests — and it is covered in full detail in Part 2 of this lesson.

Element 3 — Written Safeguards for Each Identified Risk

For every risk identified in your assessment, your WISP must describe the specific control in place to address it. The FTC Safeguards Rule identifies the categories of safeguards that must be covered:

Risk Category	Required Safeguard	Example for a Small Practice
Access control	Limit who can access client data to only those who need it	Unique login credentials per user; role-based access; no shared passwords
Data encryption	Encrypt client data in transit and at rest	Full-disk encryption on all devices; encrypted email for client document transmission
Multi-factor authentication	Require MFA on all systems accessing client data	MFA enabled on tax software, email, cloud storage, and e-Services
Physical security	Secure physical locations where data is stored or processed	Locked filing cabinets; locked office; clean-desk policy when away from workstation
Secure disposal	Destroy data no longer needed in a way that prevents recovery	Cross-cut shredder for paper; certified data destruction for old hard drives and USB drives
Software updates	Keep all systems patched and current	Automatic updates enabled on operating system, antivirus, and tax software

Risk Category	Required Safeguard	Example for a Small Practice
Backup and recovery	Maintain encrypted off-site backups and test restoration at least annually	Daily encrypted cloud backup; annual restore test documented in the WISP

Safeguards listed in your WISP must be in place today

[Image: bell-on.svg]

— not aspirational. If MFA has not yet been enabled, do not list it as a current safeguard. List it as a remediation action with a target completion date. A WISP that describes controls that do not actually exist is inaccurate — and in the event of a breach, that inaccuracy becomes a significant regulatory and legal liability.

Element 4 — Vendor and Service Provider Oversight

Your WISP must address the third parties who have access to your clients' data — your tax software vendor, cloud backup provider, email service, client portal, and any IT support provider. You are not relieved of responsibility simply because a vendor suffers the breach. Your obligation is to select vendors with reasonable security practices, include data protection requirements in your agreements, and review your vendors' security posture at least annually.

What to document: List each vendor that accesses client data, note whether they have a SOC 2 certification or published security policy, confirm that your agreement requires them to protect client data and notify you of any breach, and record the date you last reviewed their security posture. Update this list during each annual WISP review.

Element 5 — Incident Response Plan and Annual Review

Your WISP must include written procedures for what happens when something goes wrong — before it happens. The incident response plan must address how you detect and confirm a breach, who inside the practice is notified first, how and when you notify the IRS (within 24 hours), how and when you notify affected clients, and how you document the incident and response. Module 3 of this course covers incident response in full.

The WISP must also describe your annual review process: who reviews it, when, what triggers an off-cycle review, and how each review is documented. Every review must produce a dated, signed entry in Section 8 of the plan — the audit trail that demonstrates your WISP is actively maintained rather than filed and forgotten.

Part 2 — Documentation & Post-Incident Review

Step 1 — Build Your Data Inventory

The risk assessment is the diagnostic step that makes your WISP specific to your practice. It is a structured process of identifying what client data you hold, where it lives, who can reach it, and what could go wrong. For a small tax practice, a thorough risk assessment does not require outside consultants or specialized software — it requires honest, systematic answers to a defined set of questions about your own office.

Data Location	Type of Data Stored	Who Has Access
Tax software (desktop or cloud)	Returns, SSNs, financials, bank accounts	Preparers and admin staff with a login
Email inbox and sent folder	Documents clients emailed in; PDFs sent to clients	Anyone with email account credentials
Cloud storage (Drive, Dropbox, etc.)	Scanned documents, intake forms, prior returns	Anyone with the link or folder access
Local computer hard drive	Downloaded PDFs, saved client files	Anyone who can log into the computer
Paper files and folders	Printed returns, source documents, signed forms	Anyone with physical access to the office
Mobile phone	Client emails, text messages, photos of W-2s and 1099s	Phone owner; anyone who picks up an unlocked phone
USB drives or external hard drives	Backup copies of returns or client files	Anyone who physically possesses the drive
Fax machine or online fax service	Incoming source documents from clients or employers	Anyone with access to the fax output or account

Do not overlook the mobile phone.

[Image: mobile-screen-button.svg]

Do not overlook the mobile phone. Many preparers receive photos of W-2s and 1099s via text message on a personal phone with no PIN, no encryption, and no remote wipe capability. Your phone is a data storage device in scope of the Safeguards Rule and must appear in your data inventory.

Step 2 — Identify Threats

For each data location in your inventory, identify realistic threats. Threats fall into three categories:

External Threats: Phishing emails targeting your login credentials; ransomware delivered via malicious attachment or link; brute-force attacks on remote access tools; physical break-in to your office or vehicle; theft of a laptop, phone, or USB drive

Internal Threats: Current or former employee accessing data beyond the scope of their role; contractor or seasonal preparer retaining client data after their engagement ends; employee emailing client files to a personal account for convenience.

Accidental and Environmental Threats: Client document emailed to the wrong recipient; client file left in a public place; hardware failure without an off-site backup; fire, flood, or power surge destroying local files with no recovery copy.

Step 3 — Rate Each Risk

Rate each identified risk on two dimensions — likelihood and impact — using Low, Medium, or High. The combination tells you where to focus your safeguard implementation first. Do not rate everything as Low to minimize the work — an assessment that finds no significant risks is not credible and does not satisfy the Safeguards Rule.

Risk	Likelihood	Impact	Priority Action
Phishing email captures login credentials	High	High	Immediate — enable MFA on all systems
Laptop stolen from vehicle	Medium	High	High — full-disk encryption required
Email sent to wrong client	Medium	Medium	Medium — double-check recipient procedure
Former employee retains system access	Medium	High	High — formal offboarding checklist required
Paper file left unsecured in office	Medium	Medium	Medium — clean-desk policy required
USB drive lost or stolen	Low	High	High — encrypt all removable media
No off-site backup — local files destroyed	Low	High	High — encrypted cloud backup required

Step 4 — Document the Assessment

The risk assessment must be written down and retained as part of your WISP. It does not need to be elaborate — a data inventory table, a threat and rating table like the one above, and a brief narrative describing your process is fully sufficient for a small practice. What regulators look for is evidence that you: identified the data you hold, identified realistic threats to that data, evaluated likelihood and impact honestly, and used the results to

drive the safeguards written into your plan.

Your risk assessment must be updated whenever your practice changes.

[Image: bell-on.svg]

Adding a new employee, switching tax software platforms, moving to a cloud-based workflow, or opening a second office location all introduce new risks. The FTC requires re-assessment at any material change to operations — not just at the annual review. Document each update with a date.

Part 2 — Documentation & Post-Incident Review

Scenario — Building a Compliant WISP for a Solo EA

[Image: scene-scaled.webp]

Patricia is a solo EA who prepares approximately 150 individual returns annually from a home office. She uses one desktop computer, cloud-based tax software, a cloud backup service, and a cross-cut shredder. She has no employees. Here is how her WISP addresses all five elements:

- **Element 1 — Coordinator:** Patricia, EA — sole proprietor and Information Security Coordinator. Reports to herself as firm owner; documents annual review in Section 8 each October.
- **Element 2 — Data Inventory and Risk Assessment:** Client SSNs, DOBs, W-2/1099 data, bank accounts stored in cloud tax software and encrypted cloud backup. Mobile phone receives client document photos. Primary risks rated: phishing (High/High), device theft (Medium/High), accidental email (Medium/Medium).
- **Element 3 — Safeguards:** Full-disk encryption enabled on desktop; MFA enabled on tax software, email, and cloud backup; strong unique passwords via password manager; paper documents shredded after scanning; phone has PIN lock and remote wipe enabled; office door locked when unattended.
- **Element 4 — Vendors:** Cloud tax software vendor (SOC 2 certified, reviewed annually); cloud backup provider (security policy reviewed); email provider (MFA

required; data processing agreement in place). All vendor agreements reviewed for data protection language each October.

- **Element 5 — Incident Response and Review:** IRS Stakeholder Liaison number posted on printed breach response card. Annual review each October before filing season preparation begins. Post-breach WISP update triggered by any security incident regardless of timing.

Common Errors

- Completing the risk assessment once and never updating it — it must be reviewed annually and after any material change to the practice.
- Omitting mobile devices from the data inventory — phones and tablets that receive client documents are fully in scope.
- Rating all risks as Low to minimize the remediation work — an honest assessment is the only kind that protects you legally and operationally.
- Listing safeguards that are planned but not yet in place — the WISP must reflect current reality, not aspirational goals.
- Failing to connect assessment findings to specific safeguards in the plan — the assessment is only useful if it drives documented action.

2.2 - Employee Training Requirements

[Image: training.webp]

Lesson at a Glance

Technology safeguards stop many threats — but human error remains the leading cause of tax preparer data breaches. A WISP that addresses technical controls while ignoring staff training is incomplete. The FTC Safeguards Rule requires that all personnel with access to client information receive security awareness training. For tax practices, this means every person who touches taxpayer data — full-time preparers, part-time staff, seasonal employees, and contractors — must be trained on the firm's security policies and their personal responsibilities. The training must be documented. This lesson explains what training must cover, how to deliver it proportionally, and how to record it in a way that satisfies regulators.

Learning Objectives

After completing this lesson you will be able to:

- Identify who in your practice must receive security awareness training.
- Describe the minimum content required in annual staff security training.
- Implement a training process appropriate to the size of your practice.

- Create a training log that documents compliance with the Safeguards Rule requirement.

Who Must Be Trained

The FTC Safeguards Rule applies the training requirement to all personnel — a term that covers everyone who has access to client information in the course of their work for your practice:

- Full-time and part-time preparers
- Administrative and front-desk staff who handle intake forms or client calls
- Seasonal or temporary employees hired during filing season
- Independent contractors who access your systems or client files
- Remote workers accessing the firm's network or cloud storage

Seasonal employees are frequently overlooked.

[Image: siren-on.svg]

A preparer hired for January through April may work with hundreds of client files. They must receive security training before they are given access to any client data — not after filing season ends. Training a seasonal employee on their first day is not ideal but is far better than never training them at all. Document the training date in your log regardless of timing.

Who Must Be Trained

Your WISP's training section must describe the topics covered in annual security training. At minimum, training should address:

Topic	What Employees Need to Know
Phishing recognition	How to identify suspicious emails; never click links or open attachments from unknown senders; verify requests for credentials or wire transfers by phone
Password policies	Firm's password requirements (length, complexity, no reuse); use of a password manager; never share passwords with colleagues or write them down
Multi-factor authentication	Why MFA is required; how to use it on firm systems; what to do if an MFA prompt appears when the employee did not initiate a login

Topic	What Employees Need to Know
Device security	Lock screen when stepping away; never leave a laptop unattended in a vehicle; report lost or stolen devices immediately
Data handling	Never email client documents from a personal account; never store client files on personal devices; shred documents rather than recycling or trashing
Breach reporting	How to recognize a potential breach (suspicious activity, ransomware notice, missing device); who to notify immediately; do not attempt to investigate alone
Access control	Do not share login credentials; do not access client files beyond what is needed for your assigned work; report access that seems broader than necessary

How to Deliver Training in a Small Practice

The FTC Safeguards Rule does not prescribe a delivery method — it requires that training occur and be documented. Practical delivery options for small tax practices include:

- **Annual staff meeting:** Walk through the firm's WISP with all staff before the filing season begins. Review any changes from the prior year. Q&A included. Duration: 30–60 minutes.
- **Written acknowledgment:** Provide each employee with a printed or emailed summary of the firm's security policies. Require a signed (or emailed) acknowledgment that they have read and understood the policies.
- **Third-party online training:** Several CE providers and cybersecurity vendors offer short security awareness courses (often 30–60 minutes) that generate a completion certificate. This is a strong option for multi-preparer firms.
- **IRS resources:** The IRS Security Summit produces free, preparer-specific security training materials each year. These can serve as the basis for your annual training meeting.

Documenting Training — The Training Log

Your WISP must reference a training log, and the log itself should be maintained as a supporting document. A simple training log includes:

- Employee name and role
- Date of training
- Topics covered (or title of course completed)
- Employee signature or electronic acknowledgment
- Name of trainer or training provider

Who Must Be Trained

Sample Training Log Entry

Employee	Role	Training Date	Topics / Course	Acknowledgment
Robyn	Tax Preparer	01/08/2026	Annual WISP Review: phishing, MFA, device security, breach reporting	Signed 01/08/2026
Anita	Admin Staff	01/08/2026	Annual WISP Review: phishing, MFA, device security, breach reporting	Signed 01/08/2026
Mona	Seasonal Preparer	01/15/2026	New hire security orientation: WISP overview, password policy, data handling	Signed 01/15/2026

Practitioner Tips

- **Tie training to your annual WISP review.** Schedule both for the same time each year — October or November works well for most practices, giving you time to update the plan and train staff before filing season begins in January.
- **For solo preparers:** You still need to document your own annual training. Completing an IRS Security Summit webinar or a CE course on data security each year satisfies this requirement and creates a dated record.
- **Make phishing the focus.** Post-breach investigations consistently show that phishing is the entry point for the majority of tax preparer breaches. Even 15 minutes on how to recognize a phishing email — with real examples — can dramatically reduce your risk.
- **Update training content when threats evolve.** The IRS releases new scam alerts regularly. When a new phishing campaign targeting tax preparers is announced, share it with your staff immediately — don't wait for the annual training cycle.

2.3 - WISP Template Walkthrough

[Image: template.webp]

Lesson at a Glance

The IRS Security Summit publishes a free WISP template specifically designed for tax professionals. It is the most practical starting point available for small and solo practices. This lesson walks through the template section by section — explaining what each part

requires, what the most common mistakes are when completing it, and what customization is absolutely necessary to make it a compliant, practice-specific document rather than a generic placeholder. By the end of this lesson, you will know exactly what to write in each section of the IRS template to produce a finished, compliant WISP for your practice.

- Locate and access the current IRS Security Summit WISP template
- Identify each major section of the template and its required content.
- Customize the template with practice-specific information that makes it compliant.
- Recognize the sections most commonly left incomplete — and understand why they matter most.

Where to Find the Template

The IRS Security Summit WISP template is available at **IRS.gov** under the "Protect Your Clients" section. The IRS updates the template periodically — always use the most current version. As of the time this course was written, the template is a fillable Word document that can be saved, customized, printed, and stored electronically.

Checklist for Safeguarding Taxpayer Data

Instructor note: This HTML checklist is adapted from the IRS “Checklist for Safeguarding Taxpayer Data.” Use it as an on-screen modal, course handout, or WISP training checklist.

Administrative Activities

Checklist Item	Ongoing	Done	N/A
Complete a Risk Assessment. Identify the risks			

Checklist Item	Ongoing	Done	N/A
and potential impacts of unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that can be used to access taxpayer data. How vulnerable is your customer's data to theft, disclosure, unauthorized alterations or unrecoverable loss? What can you do to reduce the impact to your customers and your business in such an event? What can you do to reduce vulnerability?			
Write and follow an Information Security Plan that: • Addresses every item identified in the risk assessment. • Defines safeguards you want affiliates and service providers to follow.			

Checklist Item	Ongoing	Done	N/A
• Requires a responsible person to review and approve the Information Security Plan. • Requires a responsible person to monitor, revise, and test the Information Security Plan on a periodic, recommended annual, basis to address any system or business changes or problems identified.			
Periodically, recommended annually, perform a Self-Assessment to: • Evaluate and test the security plan and other safeguards you have in place. • Document information safeguards deficiencies.			

Checklist Item	Ongoing	Done	N/A
Create and execute a plan to address them.			
Retain a copy of the Self-Assessment and ensure it is available for any potential reviews.			
If required by the FTC Privacy Rule, provide privacy notices and practices to your customers.			
Specify in contracts with service providers the safeguards they must follow and monitor how they handle taxpayer information.			
Ask service providers to give you a copy of their written security policy on safeguarding information.			

Facilities Security

Checklist Item	Ongoing	Done	N/A
Protect from unauthorized access and potential danger, for example theft, floods and tornados, all places where taxpayer information is located.			
Write procedures that prevent unauthorized access and unauthorized processes.			

Checklist Item	Ongoing	Done	N/A
Assure that taxpayer information, including data on hardware and media, is not left unsecured on desks or photocopiers, in mailboxes, vehicles, trashcans or rooms in the office or at home where unauthorized access can occur.			
Authorize and control delivery and removal of all taxpayer information, including data on hardware and media.			
Lock doors to file rooms and/or computer rooms.			
Provide secure disposal of taxpayer information, such as shredders, burn boxes or temporary file areas until it can be securely disposed.			

Personnel Security

Checklist Item	Ongoing	Done	N/A
Create and distribute Rules of Behavior that describe responsibilities and expected behavior regarding computer information systems as well as paper records and usage of taxpayer data. Have all information system users complete, sign, and submit an acknowledgement that they have read, understood, and agree to comply with the rules of behavior. An example of rules of behavior can be found in Appendix A of NIST SP-800 18 Guide for Developing Security Plans for Federal Information Systems.			
Ensure personnel from third-party providers such as service bureaus, contractors, and other businesses providing information technology services meet the same security requirements as those applied to your personnel.			
Address Rules of Behavior for computer system management.			
When interviewing prospective personnel, explain the expected Rules of Behavior.			
When possible, perform a background and/or reference check on new employees who will have contact with taxpayer information. Conduct background screenings that are appropriate to the sensitivity of an assigned position.			
Screen personnel prior to granting access to any paper or electronic data. This will help ensure their suitability for a position requiring confidentiality and trust.			
Have personnel who will have access to taxpayer information sign nondisclosure agreements on the use of confidential taxpayer information.			

Checklist Item	Ongoing	Done	N/A
Develop and enforce formal compliance policies and processes, including possible disciplinary action, for all personnel who do not comply with the business's established information security policies and procedures.			
Terminate access to taxpayer information, for example login IDs and passwords, for those employees who are terminated or who no longer need access.			
For each employee who is terminated, conduct an exit interview and ensure the employee returns property that allows access to taxpayer information, for example laptops, media, keys, identification cards and building passes.			
Train staff on Rules of Behavior for access, non-disclosure and safeguards of taxpayer information. Provide refresher training periodically.			

Information Systems Security

Information systems include both automated and manual systems made up of people, machines and/or methods for collecting, processing, transmitting, storing, archiving and distributing data. To help ensure the accuracy, validity, consistency and reliability of taxpayer data, you should manage taxpayer data information systems based on the guidelines below.

Checklist Item	Ongoing	Done	N/A
Grant access to taxpayer information systems only on a valid need-to-know basis that is determined by the individual's role within the business.			
Put in place a written contingency plan to perform critical processing in the event that your business is disrupted. It should include a plan to protect both electronic and paper taxpayer information systems. Identify individuals who will recover and restore the system after disruption or failure.			
Periodically test your contingency plan.			
Back up taxpayer data files regularly, for example daily or weekly, and store backup information at a secure location.			
Maintain hardware and software as needed and keep maintenance records.			

Computer Systems Security

Checklist Item	Ongoing	Done	N/A
Identify and authenticate computer system users who require access to electronic taxpayer information systems before granting them access.			
Manage user identities by: • Identifying authorized users of electronic taxpayer information systems and grant specific access rights/privileges. • Assigning each user a unique identifier. • Verifying the identity of each user. • Disabling user identifiers after an organization-defined time period of inactivity. • Archiving user identities.			

Checklist Item	Ongoing	Done	N/A
Implement password management procedures that require strong passwords.			
Require periodic password changes.			
Disable and remove inactive user accounts.			
Protect electronic taxpayer information systems connected to the Internet with a barrier device, for example firewall, router or gateway. Any failure of these devices should not result in an unauthorized release of taxpayer data.			
When storing taxpayer information electronically, consider following best practices and store it on separate secure computers or media that are not connected to a network and that are password protected and encrypted.			

Checklist Item	Ongoing	Done	N/A
Encrypt taxpayer information when attached to email.			
Encrypt taxpayer information when transmitting across networks.			
Regularly update firewall, intrusion detection, anti-spyware, anti-adware, anti-virus software and security patches.			
Monitor computer systems for unauthorized access by reviewing system logs.			
Lock out computer system users after three consecutive invalid access attempts.			
Remove all taxpayer information once the retention period expires by using software designed to securely remove data from computers and media prior to disposing of hardware or media. The FTC Disposal Rule has information on how to dispose of sensitive data.			

Checklist Item	Ongoing	Done	N/A
As recommended by the FTC, reduce risks to computer systems by performing vulnerability scans and penetration tests periodically. You can learn more about this at the FTC website in their article “FTC Facts for Business – Security Check: Reducing Risks to Your Computer Systems.”			

Media Security

Checklist Item	Ongoing	Done	N/A
Store computer disks, removable media, tapes, compact disks, flash drives, audio and video recordings of conversations and meetings with taxpayers, and paper documents in a secure location, cabinet, or container.			
Secure media storage areas, including rooms, cabinets and computers by locks or key access. Where appropriate, employ an automated mechanism to ensure only authorized access.			
Restrict authorized access to media storage.			
Limit removal of taxpayer information to authorized persons and perform information access audits regularly.			
Securely remove all taxpayer information when disposing of computers, diskettes, magnetic tapes, hard drives, or any other electronic media that contain taxpayer information. The FTC Disposal Rule has information on how to dispose of sensitive data.			
Shred or burn paper documents before discarding them.			

Certifying Information Systems for Use

Checklist Item	Ongoing	Done	N/A
Determine if risks are acceptable to certify systems for use.			
Sign an authority to operate.			
If you use a certified independent certification company, consider the following: • On a periodic, recommended annual, basis, have an independent individual or business with relevant security expertise evaluate the security plans, controls, and any other safeguards implemented in your business against best practices. • Have a report generated from the audit that certifies that your			

Checklist Item	Ongoing	Done	N/A
business follows best practices. • Ensure the report highlights any deficiencies and provides recommendations for their correction. • Develop a plan for your business to correct any deficiencies found and to ensure that the plan is successfully executed. • Retain a copy of the audit report to ensure it is available for any potential reviews. • Be prepared to show how you mitigate risks.			

Your Can Review the Template by Clicking here

[Image: wisp_icon.webp]

Save your completed WISP in two places: one electronic copy (encrypted, backed up off-site) and one printed copy kept in a secure location in your office. Name the file with your firm name and the date completed — for example, "Smith Tax Services WISP 2026-01-15.docx."

Section-by-Section Walkthrough

Section 1 — Firm Information and Coordinator Designation

This section establishes the identity of your practice and names the person responsible for the plan.

What to fill in: Firm name, business address, PTIN or EIN, the full name and contact information of your Information Security Coordinator, and the date the plan was created or last reviewed.

Common mistake: Leaving the coordinator line blank or writing "owner" without a name. A name is required — the plan must identify a specific, reachable individual.

Section 2 — Data Inventory

This section lists the types of client information your practice collects and where that information is stored.

What to fill in: Use the categories from your risk assessment (Lesson 2.2). List electronic data locations (tax software, email, cloud storage, local drives) and physical data locations (paper files, filing cabinets). For each location, note who has access.

Common mistake: Listing only the tax software and ignoring email, mobile devices, and paper files. All three forms of data — electronic, physical, and transmitted — must be addressed.

Section 3 — Risk Assessment Summary

This section lists the types of client information your practice collects and where that information is stored.

What to fill in: Use the categories from your risk assessment (Lesson 2.2). List electronic data locations (tax software, email, cloud storage, local drives) and physical data locations (paper files, filing cabinets). For each location, note who has access.

Common mistake: Listing only the tax software and ignoring email, mobile devices, and paper files. All three forms of data — electronic, physical, and transmitted — must be addressed.

Section 4 — Safeguards

This is the largest section of the template and the one that must be most thoroughly customized. It asks you to describe the specific safeguards your practice has in place for each category of risk.

Safeguard Category	What to Document
Access control	Unique credentials per user, role-based access, MFA enabled on all systems with client data
Encryption	Full-disk encryption on all laptops and desktops; encrypted email for transmitting client documents; encrypted cloud storage
Physical security	Locked office, locked filing cabinets, clean-desk policy, visitor sign-in procedure if applicable
Secure disposal	Cross-cut shredder for paper; certified destruction or degaussing for old hard drives and USB drives
Software and updates	Automatic OS and software updates enabled; firewall active; antivirus/anti-malware installed and current
Remote access	VPN required for remote work; no public Wi-Fi for accessing client data without VPN
Backup and recovery	Daily encrypted backup to off-site or cloud location; recovery tested annually

Common mistake: Writing what you plan to do rather than what you currently have in place. If MFA is not yet enabled, do not list it as a current safeguard — list it as a remediation item with a completion date. The plan must be accurate.

Section 5 — Vendor Management

This section lists your key vendors and documents how you verify their security practices.

What to fill in: Name each vendor that has access to client data (tax software, cloud backup, email, payroll platforms). Note whether each has a published security policy, SOC 2 certification, or signed data protection agreement. Note the date you last reviewed their security posture.

Common mistake: Omitting the email provider. Email is the primary method most tax preparers use to transmit and receive client documents — it is the most vulnerable channel and must be addressed.

Section 6 — Employee Training

This section documents your training program and references your training log.

What to fill in: Describe your annual training process (meeting, online course, written acknowledgment), the topics covered, and the frequency. Reference your training log as a supporting document.

Section 7 — Incident Response Plan

This is the most commonly incomplete section in small-practice WISPs — and the one regulators examine first after a breach.

What to fill in: Step-by-step procedures for detecting, containing, reporting, and documenting a breach. Include the IRS Stakeholder Liaison contact information for your area. Specify the 24-hour IRS notification requirement. Name the person who notifies clients and how. Module 3 of this course covers incident response in full detail.

Section 8 — Annual Review

This section documents your commitment to reviewing and updating the plan each year.

What to fill in: The date of your most recent review, the name of the person who conducted it, a summary of any changes made, and the scheduled date of the next review. Each time you update the plan, add a new entry to this section rather than overwriting the prior one — this creates an audit trail.

Final Checklist Before You Sign

- Every blank in Sections 1–8 is filled in with practice-specific information
- No section reads "N/A" or "See above" without a genuine reason
- The incident response plan names a real person and includes IRS contact information
- The vendor list is current and complete
- The safeguards listed are in place today — not aspirationalThe plan is dated and signed by the firm owner or coordinator

3.1 - Identifying a Data Breach

[Image: databreach.webp]

Lesson at a Glance:

A data breach is any event in which client information is accessed, used, disclosed, or destroyed without authorization — or in which authorized access results in data being put at risk. Breaches are not always dramatic. Many begin as a subtle anomaly: an unfamiliar login, a client who reports a duplicate return filed in their name, a ransomware notice on a screen. The ability to recognize a breach — or a suspected breach — quickly is critical, because the IRS requires notification **within 24 hours of discovery.** This lesson covers the

warning signs of a breach, how to distinguish a confirmed breach from a suspected one, and the immediate steps to take the moment you believe your system has been compromised.

Learning Objectives

After completing this lesson you will be able to:

- Define a data breach in the context of a tax preparation practice.
- Identify the most common warning signs that a breach has occurred or is in progress.
- Distinguish between a confirmed breach and a suspected breach — and explain why both require action.
- Describe the immediate containment steps to take upon discovering a breach.

What Counts as a Data Breach

For tax preparers, a data breach includes any of the following:

- Unauthorized access to your tax software, email, or file storage systems
- A stolen or lost laptop, phone, USB drive, or paper file containing client information
- Ransomware that encrypts — or may have copied — client data before locking it
- An employee accessing client files beyond the scope of their role
- Client documents emailed to the wrong recipient
- A vendor breach that exposed data your practice stored with that vendor
- A client reporting a fraudulent return filed in their name — which may indicate your system was the source of the stolen data

suspected breach requires the same immediate action as a confirmed one

[Image: lock-keyhole-open.svg]

You do not need to wait for certainty before notifying the IRS. The 24-hour notification window begins at discovery of a suspected breach — not confirmation. Acting on a suspicion that turns out to be a false alarm is far better than delaying notification while you investigate and missing the reporting deadline.

Warning Signs of a Breach

Many tax preparer breaches are discovered not through monitoring systems but through external signals — a client call, a software alert, or an IRS notice. Train yourself and your staff to recognize these indicators immediately:

Warning Sign	What It May Indicate	Immediate Action
Client reports a duplicate return filed in their name	Your client data was used to file a fraudulent return — possibly from a breach of your system	Contact IRS Stakeholder Liaison; do not file the legitimate return electronically until resolved
Unexpected IRS e-Services login from an unrecognized device or location	Credential theft — someone has your e-Services username and password	Change credentials immediately; enable MFA if not already active; notify IRS
Tax software generates returns you did not prepare	Attacker has access to your software account and is filing fraudulent returns	Disconnect from internet; contact software vendor; notify IRS
Ransomware notice on your screen	Ransomware infection — all local files may be encrypted; data may also have been copied before encryption	Disconnect from internet immediately; do not pay the ransom; contact IRS and law enforcement
Antivirus detects malware or unusual outbound network traffic	Malware may be exfiltrating data from your system	Isolate the affected device; contact your IT provider or software vendor
Client receives phishing email appearing to come from your office	Your email account may be compromised, or your domain is being spoofed	Change email credentials; enable MFA; notify affected clients; investigate email account access logs
Missing paper file or client folder	Physical data breach — data may have been taken intentionally or lost	Document what was missing; assess which clients are affected; begin breach response

Immediate Containment Steps

The moment you suspect a breach, your priority is containment — stopping the bleeding before assessing the full extent of the damage. The following steps apply to most breach scenarios:

- **Disconnect the affected device from the internet.** Unplug the ethernet cable or turn off Wi-Fi. This stops an active attacker from continuing to access or exfiltrate data. Do not turn the device off — powering down can destroy forensic evidence.
- **Do not attempt to investigate or "fix" the breach yourself.** Clicking around on a compromised system, deleting files, or reinstalling software can destroy the evidence needed to determine what happened and which clients are affected.
- **Document everything immediately.** Write down the date and time you discovered the issue, what you observed, and every action you have taken. This log is your incident documentation — it will be needed for IRS reporting, client notification, and any regulatory inquiry.
- **Change passwords for all systems that may have been accessed.** Start with tax software, e-Services, email, and cloud storage. Do this from a device that was not affected.
- **Contact your tax software vendor.** Most major tax software providers have a dedicated security or fraud response line. They can help identify whether fraudulent returns were filed through your account and can flag your EFIN.

Keep a printed breach response card in your office

[Image: siren-on.svg]

In a real breach — especially a ransomware attack — your computer may be inaccessible. A laminated card with the IRS Stakeholder Liaison phone number, your software vendor's fraud line, and the first six steps of your incident response plan ensures you can act even when your systems are down.

Scenario 1 — The Client Call

[Image: scene-scaled.webp]

On February 10th, a client calls to say she received an IRS notice stating her return had already been filed — but she has not yet provided her documents to her preparer, Denise.

Analysis: This is a breach indicator. Someone filed a fraudulent return using the client's data — and Denise's office is a likely source, since she holds the client's SSN and prior-year return. Denise must treat this as a suspected breach immediately: document the call, contact the IRS Stakeholder Liaison, review her system for other signs of unauthorized access, and assess whether other clients may have been affected. She cannot wait to confirm that her system was the source before acting.

Scenario 2 — The Ransomware Screen

[Image: scene-scaled.webp]

On March 3rd, a preparer arrives at the office and finds a ransomware notice on the office computer. The screen demands payment in cryptocurrency within 72 hours to restore access to encrypted files.

Analysis: This is a confirmed breach. The preparer should immediately unplug the computer from the network (do not shut it down), notify the IRS Stakeholder Liaison, contact local law enforcement and the FBI's Internet Crime Complaint Center (IC3.gov), and contact their tax software vendor. They should not pay the ransom — payment does not guarantee file restoration and does not address the likelihood that data was copied before encryption. All clients whose data was on the affected system must be treated as potentially compromised.

Common Errors

- Waiting for certainty before acting — the 24-hour IRS notification clock starts at suspected breach, not confirmed breach.
- Turning off the affected computer — this destroys forensic evidence needed to determine scope.
- Failing to change credentials on all systems, not just the one directly affected.
- Not documenting actions taken during the first hours — this log is critical for regulatory reporting.

3.2 - Incident Response Plan Step-by-Step

[Image: Incident-Response.webp]

Lesson at a Glance

An incident response plan is the written, step-by-step procedure your practice follows from the moment a breach is discovered through containment, notification, remediation, and documentation. It is required in your WISP — and it must be understood before a breach occurs, not read for the first time during one. This lesson walks through each phase of the response in sequence, explains what must happen within the IRS's **24-hour notification window**, and provides the specific contacts and actions needed at each stage. The goal is that any person in your office — not just the coordinator — can execute the plan if needed.

Learning Objectives

After completing this lesson you will be able to:

- Execute each phase of an incident response from discovery through post-incident review.
- Meet the IRS 24-hour notification requirement accurately and completely.
- Identify every internal and external party who must be contacted during a breach response.
- Write the incident response section of your WISP using the framework provided in this lesson.

The Four Phases of Incident Response

A complete incident response moves through four sequential phases. Each phase has specific required actions. Skipping a phase — especially notification — creates regulatory and legal exposure.

Phase 1 — Contain (Hours 0–2)

The moment a breach is discovered or suspected, containment is the first priority. The goal is to stop the attacker from accessing additional data while preserving the evidence needed to understand what happened.

- Disconnect the affected device(s) from the internet — do not power them off.
- Revoke or change credentials for all systems that may have been accessed, from a clean, unaffected device.
- If a physical breach (stolen device, missing file), document what is missing and secure remaining physical records.
- Do not delete files, reinstall software, or attempt to clean the system — this destroys forensic evidence.
- Begin your incident log: date, time, what was observed, and every action taken.

Phase 2 — Notify (Within 24 Hours of Discovery)

This is the most time-sensitive phase. The IRS requires notification within 24 hours of discovering a suspected or confirmed breach. Notification has multiple components — all must happen within that window:

Who to Notify	How	What to Say
IRS Stakeholder Liaison	Phone — find your local contact at IRS.gov/stakeholderliaisonlocalcontacts	Firm name, EFIN, nature of breach, number of potentially affected clients, actions taken so far
Tax software vendor	Phone — use the fraud/security line, not general support	Your account credentials may be compromised; request account freeze and review of recent filings
FBI Internet Crime Complaint Center	Online report at IC3.gov	Description of the incident, type of attack, estimated scope
Local law enforcement	Non-emergency line or in person for physical breaches	File a police report — the report number may be required for insurance and state notifications
Your state tax agency	Phone or online — most states have a separate breach notification requirement	Same information as IRS notification; check your state's specific requirements
Your cyber liability insurer (if applicable)	Phone — most policies require prompt notification	Nature and scope of breach; actions taken; request guidance on coverage

[Image: clock-desk.svg]

The 24-hour clock is firm. The IRS has stated clearly that notification should occur within 24 hours of discovery of a suspected breach — not after you have confirmed every detail, not after you have finished investigating, and not after you have notified clients. The IRS notification comes first. Client notification comes next, typically within 2–3 business days depending on your state's breach notification law.

Phase 3 — Assess and Remediate (Days 1–14)

Once containment is in place and notifications have been made, the focus shifts to understanding the full scope of the breach and restoring secure operations.

- **Determine scope:** Which clients' data was potentially accessed? Use your data inventory (from your WISP) to identify every client whose records were stored on the affected system or account.
- **Engage a forensic professional if needed:** For ransomware attacks or network intrusions, an IT forensics professional can determine exactly what data was accessed and when. This information is critical for accurate client notification.
- **Restore from backup:** Once the affected system has been forensically examined, wipe and restore from your most recent clean backup. Test the restored system before reconnecting to the internet.
- **Remediate the vulnerability:** Identify how the attacker gained access and fix the gap — whether that is enabling MFA, patching software, revoking a former employee's credentials, or replacing a compromised device.
- **Notify affected clients:** Once you have identified the affected client list, send written notification. See Lesson 3.4 for what to say and how to say it.

Phase 4 — Document and Review (Within 30 Days)

After the immediate crisis is resolved, your WISP requires a post-incident review and documentation update. This is not optional — it is how you demonstrate to regulators that you responded appropriately and took corrective action.

- Finalize your incident log with a complete timeline from discovery through resolution.
- Document the root cause: how did the breach occur?
- Document every notification made: to whom, on what date, by what method.
- Update your WISP to address the vulnerability that was exploited.
- Update your risk assessment to reflect the new risk landscape post-breach.
- Conduct a staff debrief: what did your team do well? What needs to change?

Your Incident Response Quick-Reference Card

The following information should be printed and kept accessible in your office — not stored only on the computer that may be compromised during a breach:

Contact	Number / URL	When to Call
IRS Stakeholder Liaison (your local contact)	[Image: localcontacts] Scan for IRS Contacts	Within 24 hours of discovery
Tax software vendor fraud line	[Your vendor's number — fill in before a breach occurs]	Within 24 hours of discovery
FBI IC3	IC3.gov	Within 24 hours of discovery
Local law enforcement	[Your local non-emergency number]	Within 24 hours for physical breaches; same day for ransomware
Your state tax agency security contact	[Your state's contact — look up before a breach occurs]	Within 24–48 hours depending on state law
Cyber liability insurer	[Your policy number and claims line]	Within 24 hours of discovery

[Image: MS-Liason.webp]

Fill in this card now — before a breach happens. Look up your IRS Stakeholder Liaison local contact, your software vendor's fraud line, and your state agency contact today. Print the completed card and laminate it. Store one copy at your desk and one in a location away from your primary workstation.

Scenario — Phishing Breach, 48-Hour Timeline

Incident Response Scenario

Phishing Breach — 48-Hour Timeline

Monday

9:00 AM — Teresa notices unauthorized tax software access from an unknown IP address. Two fraudulent returns were filed overnight.

9:05 AM — Teresa disconnects her computer from Wi-Fi and immediately begins an incident log.

9:15 AM — From her phone, Teresa changes her tax software password, enables MFA, changes her email password, and changes her IRS e-Services password.

9:30 AM — Teresa contacts her tax software vendor's fraud department. The account is frozen, two fraudulent returns are identified, and the EFIN is flagged for monitoring.

10:00 AM — Teresa contacts her IRS Stakeholder Liaison and reports:

- Firm name
- EFIN
- Nature of breach
- Two confirmed fraudulent returns
- Actions already taken

11:00 AM — Teresa files a complaint with IC3.gov and files a police report with local law enforcement.

Tuesday

Teresa identifies the two affected clients connected to the fraudulent returns.

Teresa personally contacts each client, explains the breach, and advises them to obtain an IRS Identity Protection PIN (IP PIN).

Written client notification letters are sent after the phone calls.

Within 2 Weeks

Teresa updates her **Written Information Security Plan (WISP)** to require MFA on all systems.

She updates her firm risk assessment and documents the full incident timeline.

Teresa completes a 30-minute security review using IRS Security Summit materials.

The post-incident review is retained with the firm's security documentation.

3.3 - Notifying Clients, Documentation & Post-Incident Review

Lesson at a Glance:

[Image: Client Notification and Incident Documentation]

Once you have contained the breach and notified the IRS, two obligations run in parallel: **notifying affected clients promptly and correctly**, and **documenting every action taken from discovery through final resolution**.

Client notification is governed by state breach notification laws and your WISP. Documentation is your legal evidence that you responded appropriately — it is what regulators, courts, and insurers examine after the fact.

Client Notification

Explain what happened, what information may have been affected, what steps the firm has taken, and what protective actions the client should take next.

Incident File

Maintain a complete incident file showing discovery time, containment steps, IRS contact, vendor contact, client notices, law enforcement reports, and final resolution.

Post-Incident Review

Review what failed, what worked, what policies need updating, and what safeguards must be strengthened so the breach improves the security program.

Lesson Focus

This lesson covers what to say to clients, when to say it, what protective actions to recommend, how to build the incident file, and how to complete the post-incident review required by your WISP.

Part 1 — Notifying Clients

[Image: 1.svg]

Sequence and Timing

Client notification timing is governed by your state's breach notification law. Most states require written notice within 30 to 72 hours of discovery, though requirements vary. As a practical standard for tax practices, notify clients within **2 to 3 business days** of discovering the breach.

`The notification sequence is non-negotiable:`

[Image: IRS_.svg]

IRS Stakeholder Liaison

within 24 hours of discovery

[Image: laptop-code.svg]

Tax software vendor

same day, in parallel with IRS

[Image: handcuffs.svg]

Law enforcement

same day (local police and IC3.gov)

[Image: building-columns.svg]

Affected clients

within 2 to 3 business days after IRS notification

Do not notify clients before notifying the IRS. The IRS needs to open a case and coordinate with Criminal Investigation before clients begin calling in about fraudulent returns. Notifying clients first creates confusion and may interfere with the IRS investigation. IRS notification always comes first — no exceptions.

[Image: MS-Liason-859x1024.webp]

Who Must Be Notified

Client Notification Rule

Notify Clients When Data May Have Been Accessed

Notify every client whose nonpublic personal information was — or may have been — accessed without authorization. When in doubt, notify.

When in Doubt

The cost of notifying a client whose data was not accessed is far lower than the cost of failing to notify a client whose data was stolen and used for fraud.

Use Your WISP Inventory

Use your data inventory to identify every client whose records were stored on, or accessible through, the affected system during the relevant timeframe.

Practitioner Tip: Do not limit notification only to confirmed victims. If the system contained or could access client data, include those clients in your review and document the basis for your notification decision.

Required Content of the Notification Letter

What happened	Plain-language description of the breach type, when discovered, and how it occurred to the extent known
Data elements involved	Specifically name what may have been accessed: SSN, date of birth, bank account numbers, prior-year return data — be precise
What you have done	IRS notification, law enforcement report, credential resets, system remediation — demonstrate that you acted immediately
What the client should do	Specific, numbered protective actions — see list below
Your direct contact information	Phone and email — clients will have questions and must be able to reach you
Free resources available	IRS IP PIN program, FTC IdentityTheft.gov, free credit bureau freezes

Sample Client Notification Letter

[Image: letter-notification-1024x819.webp]

Send notification letters via certified mail with return receipt

Client Notification Record

Send notification letters by **certified mail with return receipt** for the most legally defensible record.

- If email is used, request a read receipt and retain the sent email with timestamp.
- Keep a copy of every client notification letter.
- Maintain a notification log showing every client notified and when notice was sent.

Retain notification letters, receipts, emails, and the client notification log in the breach file for a minimum of **seven years**.

Your Complete Incident File

Document	Purpose
Incident log (chronological)	Master timeline from discovery to resolution — the primary evidence of an appropriate, timely response
Initial discovery notes	What you observed when you first detected the breach — written at the time, never reconstructed after the fact

Document	Purpose
IRS Stakeholder Liaison call record	Date, time, liaison name, case number assigned, and guidance received
Tax software vendor call record	Actions taken on your account, fraudulent return findings, account status
Law enforcement report	Police report number and IC3.gov complaint confirmation number
Form 14039-B (if filed)	Business Identity Theft Affidavit with proof of submission — certified mail receipt or fax confirmation
Client notification letters	Copy of every letter with date sent, delivery method, and client name
Client notification log	Spreadsheet or table listing every client notified, date, method, and any follow-up actions
State notification records	Attorney general or state agency submission copies if required under your state's breach notification law
Forensic report (if applicable)	Scope of data accessed, method of entry, and timeline from IT forensics examination
Remediation record	Every corrective action taken — new credentials, MFA enabled, device replaced, software patched — with completion dates
Updated WISP	Revised written plan addressing the vulnerability that was exploited

The Post-Incident Review — Required Within 30 Days

The Post-Incident Review

Your WISP requires a structured post-incident review within **30 days** of resolving the breach. The purpose is simple: convert a crisis into a stronger security program.

The review must be documented and answer four critical questions.

1

What Happened and Why?

Identify the root cause of the incident.

- Phishing email
- Unencrypted stolen device
- Former employee retained access

- Vendor or service-provider breach

The root cause drives every other finding and corrective action.

2

Was the Response Adequate?

Compare the incident log against the written response plan.

- Were there delays?
- Were required notifications completed?
- Did staff understand their responsibilities?

Determine whether the response followed the WISP as written.

3

What Gaps Were Revealed?

Every breach exposes weaknesses in the security program.

- Backup procedures
- Email filtering
- Employee training

Identify every weakness revealed by the incident — not just the one directly exploited.

4

What Changes Are Being Made?

Create a documented remediation action plan.

- Specific corrective action
- Person responsible
- Target completion date

This remediation plan drives the required WISP update.

Required Outcome

A post-incident review is not simply a report about the breach. It is the mechanism that transforms lessons learned into stronger safeguards, updated procedures, improved training, and a more resilient WISP.

Updating Your WISP After a Breach

WISP Post-Breach Update Requirement

A Breach Requires an Immediate WISP Update

A breach is a mandatory off-cycle WISP update trigger regardless of when your annual review is scheduled. The security program must be updated immediately after the incident — not postponed until year-end.

Add New Safeguards

Update the WISP to include the specific safeguard that addresses the vulnerability that was exploited during the breach.

Revise Risk Assessment

Modify the risk assessment to reflect what the breach revealed about actual threats, weaknesses, and attack methods in your environment.

Improve Response Procedures

Update the incident response plan based on what worked effectively during the breach response — and what failed or caused delays.

Documentation Requirement

Add a dated entry to Section 8 of your WISP documenting the post-breach update. This audit trail is what regulators review when determining whether your security program is actively maintained or simply a document created once and forgotten.

Scenario — Full Response: Notification Through Post-Incident Review

[Image: Teresa-1024x683.webp]

Teresa discovers on Monday morning that her tax software was accessed overnight from an unrecognized IP address. Two fraudulent returns were filed using client data from her system. She follows her incident response plan: disconnects from the internet, changes all credentials from her phone, calls the IRS Stakeholder Liaison by 10:00 AM (within 24 hours), calls her software vendor who freezes the account, and files an IC3 report. She begins her incident log on a legal pad from the moment of discovery.

By Tuesday she has identified the two affected clients from the fraudulent returns. She calls each client personally that morning and follows up with a certified written notification letter the same day — including Form 14039 instructions, IP PIN enrollment link, and credit freeze guidance. Both calls and both letters are documented in her client notification log.

[Image: result-incident-1024x683.webp]

Within two weeks Teresa completes her post-incident review. Root cause: MFA was not enabled on her tax software account. Corrective action: MFA enabled on all six firm systems within 48 hours of discovery. WISP updated to require MFA as a mandatory control with annual verification. Risk assessment updated to rate phishing credential theft as High/High. Dated post-breach update entry added to Section 8.

Result: Teresa's documented, timely response — IRS notified in under 24 hours, clients notified within 48 hours, complete written records of every action, WISP updated within 30 days — demonstrates to regulators that she had a plan, followed it, and improved her program. The incident does not result in regulatory action.

Common Errors

[Image: common-errors-1024x683.webp]

4.1 - Annual WISP Review Checklist

Lesson at a Glance:

[Image: Annual WISP Review]

A WISP is only effective if it stays current.

The FTC Safeguards Rule requires that your information security program be reviewed and adjusted in response to changes in your business, emerging threats, and new regulatory guidance — at minimum once each year.

For most tax practices, the ideal review period is **October or November** — after the extended filing season ends and before the January filing season begins.

Why Review?

Security threats evolve constantly. Annual review ensures your WISP reflects current risks, technology, staffing, vendors, and regulatory requirements.

Best Time to Review

October and November provide a natural window to evaluate the security program before the next filing season begins.

Document the Review

The review itself must be documented. Regulators expect evidence that the WISP was reviewed, updated, and approved.

- Annual Review Checklist
- Review employee and contractor access
- Evaluate physical office security
- Review software vendors and service providers
- Verify passwords, MFA, backups, and encryption
- Review incidents, near misses, and emerging threats
- Update, sign, and date the WISP

When to Review

When to Review

The FTC Safeguards Rule requires review of your WISP **at least annually** and whenever a material change occurs within your practice.

Material changes require an immediate off-cycle WISP update rather than waiting for the next annual review.

Annual Review

Conduct a complete review of the WISP at least once each year to ensure policies, safeguards, vendors, employee access, and security controls remain current.

Off-Cycle Review

Significant business, technology, staffing, or security changes require immediate updates to the WISP rather than waiting until the next scheduled review.

- Off-Cycle WISP Update Triggers
- Hiring or terminating a staff member with access to client data
- Changing tax software, cloud storage, or major technology platforms
- Moving offices or implementing remote work arrangements
- Experiencing a data breach or security incident
- Significant IRS Security Summit or FTC regulatory updates
- Adding new services such as payroll, bookkeeping, or other data-intensive offerings

Best Practice

Put your annual WISP review on the calendar today. For most tax practices, **October 15** is an ideal recurring review date because it falls immediately after the extended filing deadline and before preparation begins for the next filing season.

A WISP reviewed every October is a WISP that is always ready.

Put your annual review on the calendar today

Best Practice

Put your annual WISP review on the calendar today.

- Schedule it as a recurring annual appointment.
- October 15 works well for most practices because it falls immediately after the extended filing deadline.
- The review is completed before preparation begins for the next filing season.

A WISP reviewed every October is a WISP that is always ready.

The Complete Annual Review Checklist

Annual WISP Review Checklist

Sections 1–2: Firm information, coordinator, and data inventory.

Section 1 — Firm Information & Coordinator

- Firm name, address, PTIN/EIN are current and accurate.
- The named Information Security Coordinator is still correct.
- Coordinator phone and email are current.
- A backup coordinator is named and contact information is current.
- The designation is dated with this year's review date.

Section 2 — Data Inventory

- All current software platforms and cloud accounts are listed.
- Platforms added or removed since the last review have been updated.
- All devices that store or access client data are listed, including mobile phones and home computers.
- Physical data locations such as filing cabinets and off-site storage are current.
- Access permissions have been reviewed and no former employees or inactive contractors retain access.

The Complete Annual Review Checklist

Annual WISP Review Checklist

Sections 3–4: Risk assessment and safeguards.

Section 3 — Risk Assessment

- New risks introduced since the last review have been identified and rated.
- Risk ratings reflect the current practice environment, not last year's setup.
- Risks that became incidents have been updated with actual impact information.
- Recent IRS Security Summit threat alerts have been reviewed and incorporated where appropriate.

Section 4 — Safeguards

- Multi-factor authentication is enabled on all systems containing client data.
- Full-disk encryption is enabled on all devices accessing client information.
- Antivirus and anti-malware software are current.
- Operating systems and tax software are fully updated and patched.
- Password policies reflect current best practices and password manager usage.
- Physical security measures remain in place and are being followed.
- Secure disposal procedures for paper and electronic media are active.
- Backup procedures have been verified and a restore test has been performed during the year.

The Complete Annual Review Checklist

Annual WISP Review Checklist

Sections 5–6: Vendor management and employee training.

Section 5 — Vendor Management

- Vendor list is current and includes all vendors that had access to client data during the year.
- New vendors added since the last review have been evaluated for security practices.
- Terminated vendors have been removed and confirmed to have deleted client data where required.
- Each vendor's security posture has been reviewed (SOC reports, security policies, or equivalent documentation).

Section 6 — Employee Training

- Annual security awareness training was completed and documented.
- All current employees and seasonal staff appear in the training log for the current year.
- Training materials have been updated to address new IRS Security Summit threats and guidance.

- New employees received security orientation before being granted access to taxpayer information.

Practitioner Tip

Vendor oversight and employee training are two of the most commonly reviewed areas during compliance examinations. Keep documentation for both. If it isn't documented, regulators may assume it never happened.

The Complete Annual Review Checklist

Annual WISP Review Checklist

Sections 7–8: Incident response plan and annual review record.

Section 7 — Incident Response Plan

- IRS Stakeholder Liaison contact information has been verified and updated.
- Tax software vendor fraud hotline and emergency contacts are current.
- Incident response procedures reflect lessons learned from any security incidents during the year.
- Breach notification letter templates have been reviewed and updated.
- Printed breach response quick-reference cards contain current contact information.

Section 8 — Annual Review Record

- Review date, reviewer name, and summary of changes have been documented.
- Updated WISP has been signed and dated by the owner or Information Security Coordinator.
- Previous version of the WISP has been archived and retained.
- Updated WISP has been stored in both encrypted electronic form and printed form.

Review Complete

Once all eight sections have been reviewed, updated, signed, dated, and archived, your WISP review is complete for the year.

- Retain documentation of the review.
- Archive prior versions rather than deleting them.
- Schedule next year's review before closing the file.

The Complete Annual Review Checklist

Annual WISP Review Checklist

Verify each item and document any updates made during the review.

Section 1 — Firm Information & Coordinator

- Firm name, address, PTIN and EIN are current.
- Information Security Coordinator is still correct.
- Coordinator contact information is current.
- Backup coordinator is designated and current.
- Designation updated with this year's review date.

Section 2 — Data Inventory

- All software and cloud platforms are listed.
- New and removed platforms have been updated.
- All devices including remote devices are listed.
- Physical storage locations are current.
- Former employees and contractors no longer have access.

Suggested Use

Print this checklist, complete it during the annual review, and retain it with the WISP as evidence that the review was performed and documented.

Documenting the Annual Review

Every annual review must leave a written record. At minimum, add an entry to Section 8 of your WISP that states:

- The date the review was conducted
- The name of the person who conducted it
- The date the updated plan was signed

Sample Annual Review Entry for Section 8 of Your WISP

[Image: clock-desk.svg]

"Annual review conducted on October 22, 2026 by [Name], Information Security Coordinator. The following updates were made: (1) Vendor list updated to reflect new cloud backup provider added in March 2026; prior vendor confirmed data deletion. (2) Risk assessment updated to include remote work risks following addition of home office setup for seasonal preparer. (3) Incident response contact card updated with current IRS Stakeholder Liaison phone number. (4) Staff training completed October 15, 2026 — training log updated. No security incidents occurred during the review period. Plan signed and dated by firm owner [Name] on October 22, 2026. Next scheduled review: October 2027."

Most Commonly Outdated Sections

In small tax practices, the sections most frequently found to be out of date during an annual review are:

- **Vendor list** — software platforms and cloud services change frequently; the list is often one to two tools behind reality.
- **Coordinator contact information** — phone numbers and email addresses change; an unreachable coordinator is no coordinator at all.
- **IRS Stakeholder Liaison contact** — the IRS reorganizes and reassigns liaisons; the number in your plan from two years ago may be wrong.
- **Access permissions** — former seasonal employees and contractors frequently retain access that was never formally revoked.
- **Backup verification** — many preparers assume their backup is working because it has never failed. Test the restore at least once per year.

4.2 - Passwords + MFA + Remote Work

[Image: pwdmfaremote.webp]

Lesson at a Glance

Two of the most exploited weaknesses in small tax practice security programs are credential vulnerabilities and remote work blind spots. Weak or reused passwords remain

the most common entry point for attackers. **Multi-factor authentication** — explicitly required by the 2023 FTC Safeguards Rule update — closes that gap even when a password is stolen. Remote work and mobile devices extend your security perimeter beyond your physical office and introduce risks your WISP must address with the same rigor as the office environment. This lesson covers current password standards, the MFA requirement and how to implement it, the device security rules that apply to every device touching client data, and the remote work policies your WISP must document — all with sample language ready to use.

Learning Objectives

After completing this lesson you will be able to:

- Write a compliant password policy for your WISP based on current NIST and FTC guidance.
- Identify which systems in a tax practice require MFA under the Safeguards Rule and implement it on each.
- Apply device security requirements to laptops, desktops, mobile phones, and tablets used for client work.
- Write a remote work policy for your WISP that addresses home networks, public Wi-Fi, and physical document security.

Part 1 — Password Policies & Multi-Factor Authentication

Password guidance has changed significantly in recent years. The National Institute of Standards and Technology (NIST) Special Publication 800-63B — the current federal standard for authentication — shifted away from arbitrary complexity rules (requiring uppercase, numbers, and symbols on a 90-day rotation) toward length-first policies. The FTC Safeguards Rule aligns with this updated guidance.

Policy Element	Current Best Practice	What to Write in Your WISP
Minimum length	At least 12 characters; 15+ strongly preferred	"All passwords for systems containing client data must be a minimum of 12 characters."
Complexity	Length matters more than complexity; passphrases (four or more random words) are highly effective and easier to remember	"Passwords should be a combination of letters, numbers, and symbols or a passphrase of four or more unrelated words."
Reuse	Never reuse passwords across different systems or accounts	"No password used for a firm system may be reused for any other firm or personal account."
Rotation	Change only when there is reason to believe a password has been	"Passwords must be changed immediately upon suspicion of

Policy Element	Current Best Practice	What to Write in Your WISP
	compromised — forced arbitrary rotation leads to weaker passwords	compromise. Routine rotation is not required but is permitted."
Sharing	Never share passwords between users — each person must have unique credentials	"Sharing of passwords between staff members is prohibited. Each user must have unique login credentials for every system."
Storage	Use a dedicated password manager — never write passwords on paper or store in an unencrypted document	"All firm system passwords must be stored in an approved password manager. Writing passwords on paper or storing in plain-text documents is prohibited."

Recommended password managers for small practices:

[Image: clock-desk.svg]

Bitwarden (free for individuals, low-cost for teams), 1Password, and LastPass are widely used. A password manager solves the reuse problem automatically — staff can use unique, strong passwords for every system without memorizing them. The cost is typically under $5 per user per month.

Multi-Factor Authentication — The Required Control

The 2023 FTC Safeguards Rule update added an explicit MFA requirement: MFA must be implemented for any system that accesses customer financial information. For virtually all tax practices the answer is MFA on everything — the "equivalent alternative" exception is narrow and rarely applicable to a tax preparation business.

MFA requires a user to verify identity using two or more factors: something you know (password or PIN), something you have (phone or authenticator app code), or something you are (fingerprint or face scan). The most practical method for small practices is password plus a code from an authenticator app such as Google Authenticator, Microsoft Authenticator, or Duo. An attacker who steals a password still cannot log in without the physical device generating the code.

Where MFA Must Be Enabled

Every system in your practice that stores or accesses client data must have MFA enabled. For a typical small tax practice, this includes:

- Tax software accounts (desktop and cloud-based)
- IRS e-Services and e-file accounts
- Email accounts used to send or receive client documents
- Cloud storage accounts (Google Drive, Dropbox, OneDrive, ShareFile)
- Remote access tools (remote desktop, VPN)
- Payroll or bookkeeping platforms that contain client financial data
- Your practice management or CRM software

SMS text message codes are the weakest form of MFA

[Image: clock-desk.svg]

— they can be intercepted through SIM-swapping attacks. Authenticator apps (Google Authenticator, Microsoft Authenticator) or hardware security keys (YubiKey) provide significantly stronger protection. Where possible, use an authenticator app rather than SMS codes. For IRS e-Services specifically, the IRS requires identity verification through ID.me, which includes MFA as part of the login process.

Sample WISP Language — Password and MFA Policy

[Image: clock-desk.svg]

"[Firm Name] requires multi-factor authentication on all systems used to access, store, or transmit taxpayer information. This includes but is not limited to: tax preparation software, IRS e-Services, email accounts, and cloud storage platforms. Acceptable MFA methods are authenticator applications or hardware security keys. SMS-based codes are permitted only where authenticator app MFA is not supported by the platform. Each staff member is responsible for maintaining MFA enrollment on all assigned systems. MFA enrollment must be completed before a staff member is granted access to any client data. The Information Security Coordinator verifies MFA enrollment for all staff annually and upon each new hire onboarding."

MFA Recovery — When a Device Is Lost or Changed

Document your MFA recovery procedure in your WISP to prevent lockouts and security gaps when staff get new phones:

- Save all MFA recovery codes in the firm's password manager at setup — not after a problem occurs
- Staff must notify the coordinator immediately if an MFA-enrolled device is lost or stolen
- The coordinator revokes the compromised device's MFA session and re-enrolls on a new device using stored recovery codes
- A lost device enrolled in MFA for firm systems is a potential breach event — treat it as such per your incident response plan

Part 2 — Remote Work & Device Security

Why Remote Work Requires Specific WISP Coverage

Remote work extends your security perimeter beyond the physical office and introduces risks that are more difficult to control. The FTC Safeguards Rule applies the same data protection requirements to remote environments as to office environments — there is no reduced standard for working from home. A home router with a default password, a shared family laptop, or a client document viewed in a coffee shop are all real breach vectors that must be addressed in your written plan.

Required Remote Work Policies

Policy Area	The Rule	Sample WISP Language
Approved devices	Only firm-approved or firm-configured devices may access client data remotely	"Client data may only be accessed remotely on devices approved by the Information Security Coordinator that meet the firm's device security requirements."
Public Wi-Fi	Never access client data over public or unsecured Wi-Fi without a VPN	"Staff must not access client data over public Wi-Fi networks. A VPN is required for any remote access outside a trusted private network."
Home network	Home routers used for firm work must have strong unique passwords and current firmware	"Staff working from home must use a router with a non-default password and must keep router firmware updated. Default router credentials are prohibited."
Screen privacy	Client data on screen must not be visible to unauthorized individuals	"Staff must ensure client information on screen is not visible to household members or others when working remotely."
No shared devices	Firm devices used for client work must not be used by other household members	"Devices used to access client data must not be shared with family members or other household residents."
Physical documents	Printed client documents must be secured and shredded — not recycled or placed in household trash	"Client documents printed at a remote location must be stored securely and shredded with a cross-cut shredder before disposal."
Lost device reporting	Any device used to access client data that is lost or stolen must be reported immediately	"Loss or theft of any device used to access client data must be reported to the Information Security Coordinator within one hour of discovery."

Device Security Requirements — All Devices

Every device used to access client data — in the office or remotely — must meet these minimum requirements. Document them in your WISP and verify compliance during each annual review:

Laptops and Desktops: Full-disk encryption enabled (BitLocker for Windows, FileVault for Mac); screen lock activates automatically after no more than 5 minutes of inactivity; strong login password required; OS and software updates applied promptly with automatic updates enabled; antivirus/anti-malware installed and current; firewall enabled; no unauthorized software installed.

Mobile Phones and Tablets: Device PIN, password, or biometric lock required; full-device encryption enabled (standard on modern iOS and Android when a lock screen is active); remote wipe capability enabled (Find My iPhone / Google Find My Device); OS and app updates applied promptly; no client documents stored in unencrypted personal photo libraries; business email and documents accessed through MFA-protected apps.

The mobile phone is the most overlooked device in small-practice WISPs.

[Image: mobile-screen-button.svg]

The mobile phone is the most overlooked device in small-practice WISPs. Preparers routinely receive photos of W-2s and 1099s via text message, store them in their camera roll, and never address them in their security plan. A photo of a W-2 in an unlocked phone's unencrypted camera roll is a breach waiting to happen. Your WISP must address mobile devices explicitly — they are fully in scope under the Safeguards Rule.

VPN — When and Why

A VPN encrypts all data transmitted between a remote device and the internet, making it unreadable to anyone who might intercept it on a public or unsecured network. Your WISP must require VPN use whenever client data is accessed outside a trusted private network. Practical options for small practices include a business-grade router with VPN server functionality (staff connect back to the office network), a commercial VPN service such as NordVPN Teams or Cisco AnyConnect, or confirming that your cloud-based tax platform's own encrypted connection satisfies the requirement — verify with your vendor.

Scenario

[Image: home-office-and-remote-access-audit.webp]

During her annual WISP review, preparer Angela audits her setup against her remote work policy. She finds three gaps:

- **Gap 1:** Her home router still uses the default password from installation four years ago. *Fix: Change router credentials to a strong unique password; update firmware.*

- **Gap 2:** Her teenage son occasionally uses her laptop for schoolwork. *Fix: Create a separate limited user account for personal use; tax software and client files are accessible only under her password-protected administrator account.*
- **Gap 3:** She has no VPN — when working from her daughter's house over the holidays, she accesses client files over an unknown Wi-Fi network. *Fix: Subscribe to a business VPN service ($8/month); add VPN requirement to the WISP remote work policy.*
- All three gaps are documented in the annual review record and remediated before filing season begins. Total additional monthly cost: $8. Total time to implement: approximately 90 minutes.

Common Errors

- Listing MFA as an active safeguard in the WISP before it has actually been enabled — the plan must reflect what is in place today, not what is planned.
- Omitting mobile phones from the device security section — phones that receive client document photos are fully in scope.
- Treating a home office as equivalent to the office environment without a written remote work policy — the risks are different and the WISP must address them separately.
- Not testing MFA recovery before it is needed — staff locked out of systems during filing season because a recovery code was never saved is a preventable crisis.
- Using the same password across tax software, email, and cloud storage — a single phishing event then compromises every system simultaneously.

Final Lesson – Course Feedback & Survey

Course Feedback

Share Your Experience

Your insights help us continuously improve. Please take a brief moment to share your feedback about the cybersecurity training module below.