SAFEGUARDS MONITOR

FREE TEMPLATE · VERSION 1.0 · JULY 2026

Written Information Security Plan

A fill-in WISP template for solo and small tax and accounting firms, adapted from the IRS's own Publication 5708 and checked against the current text of the FTC Safeguards Rule.

Adapted from	IRS Publication 5708, Creating a Written Information Security Plan (Rev. 8-2024)
Checked against	16 CFR Part 314 (eCFR, live text), July 17, 2026
Published by	Safeguards Monitor · safeguardsmonitor.com · independent, not a government agency
Latest version	safeguardsmonitor.com/wisp-template · free, direct download, no email required
Fill in	The Word (.docx) version is the one to fill in; the PDF is for reading and printing

READ THIS FIRST

This template is educational, adapted from IRS Publication 5708. It is general information, not legal advice for your specific situation, and completing it does not by itself make your firm compliant. For advice on your situation, consult a qualified professional.

How to use this template

This is a fill-in **Written Information Security Plan**, the written program the FTC Safeguards Rule requires a tax practice to keep. It follows the structure of the IRS's own template, Publication 5708, with the guidance rewritten in plain English, the current rule text checked section by section, and every deliberate blank made explicit. What it is not: it is not legal advice, it is not a compliance verdict, and a filled-in template is a starting point, not proof that your program meets the rule.

Where the duty comes from

Under the Gramm-Leach-Bliley Act, the FTC's Safeguards Rule treats your firm as a financial institution; the FTC's guidance names "tax preparation firms" outright. The rule's core duty, in its own words, is to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts" (16 CFR 314.3(a)). The IRS points preparers to that duty through Publication 4557 and Publication 5708, and asks every PTIN holder to attest awareness of it on Form W-12, Line 11. This document is where the written program can live.

How the blanks work

Publication 5708 is a genuinely useful skeleton, and the IRS is honest that it is a sample: the decisions are yours. Every place this template needs a decision only your firm can make is marked with a **YOUR FIRM DECIDES** box that tells you what to decide and why. Grey "Rule anchor" lines under headings show which element of 16 CFR 314.4 a section relates to. An anchor is a map reference, not a compliance determination.

If your firm is small

The written plan itself applies at every size; there is no small-firm pass on having one. What the rule does set aside, for firms that maintain customer information on fewer than 5,000 consumers, is four specific items: the written risk assessment (314.4(b)(1)), continuous monitoring or penetration testing (314.4(d)(2)), the written incident response plan (314.4(h)), and the annual report to leadership (314.4(i)) (16 CFR 314.6). Where one of those items comes up in this template, a note says so. Everything else, including the plan, the named responsible person, the safeguards, staff training, and vendor oversight, applies to a one-person shop the same as to a ten-person firm.

A sensible order to work in

1. **Name the responsible person** in Section IV. In a solo practice, that is you.
2. **Inventory what you have**: fill Attachment E (hardware and systems) and Attachment F (who can access what).
3. **Fill the risk grid** in Section V. It turns the inventory into the risks the rest of the plan answers.
4. **Work through the policies** in Sections VI and VII, deciding each YOUR FIRM DECIDES box as you go.
5. **List your service providers** in Attachment G and check the contract question for each.
6. **Sign Section X**, then have every employee sign Attachment D.
7. **Date the review cycle**: put next year's review on the calendar and log it in Attachment H.

Keep the plan alive. Review it at least once a year and after any material change: new software, new staff, a new office, an incident. The IRS calls the WISP an evergreen document, and the review log in Attachment H is what makes yours one.

Where each rule element lives in this template

The Safeguards Rule lists nine elements a written program must include, plus a separate breach-notification duty. Publication 5708 does not map its own sections to them, so this table does.

RULE ELEMENT (16 CFR 314.4)	WHAT IT ASKS	WHERE IT LIVES HERE
(a) Qualified Individual	One named person runs the program	Section IV (the DSC)
(b) Risk assessment	Base the program on the risks you actually have	Section V
(c) Safeguards, eight of them	Access controls, inventory, encryption, secure development, MFA, disposal, change management, monitoring	Sections VI and VII; Attachments A, E, F
(d) Testing and monitoring	Check that the safeguards work	Section IX
(e) Training	Staff know the plan and the threats	Section VII, Training policy; Attachment D
(f) Service providers	Choose, bind, and reassess vendors	Section VIII; Attachment G
(g) Evaluate and adjust	Update the program as things change	Section IX; Attachment H
(h) Incident response plan	A written plan for security events (set aside under 5,000 consumers)	Attachment C
(i) Annual report	Yearly written report to the owner or board (set aside under 5,000 consumers)	Section IX
(j) Breach notification	Tell the FTC as soon as possible, within 30 days, if 500 or more consumers' unencrypted information is involved	Attachment C, contact table

Prepared by Safeguards Monitor from 16 CFR 314.4 and 314.6 (eCFR), checked July 17, 2026.

Written Information Security Plan

Everything before this page is instructions. Everything from here on is your firm's document.

Firm name	_____
Firm address	_____
Plan prepared by	_____
Effective date	_____
Last reviewed	_____

I. Objective

`Rule anchor: 16 CFR 314.3(a), the written program duty`

The objective of this Written Information Security Plan (the Plan) is to create effective administrative, technical, and physical safeguards for the Personally Identifiable Information (PII) our firm collects and retains, and to meet our duties under the Gramm-Leach-Bliley Act and the FTC Safeguards Rule, 16 CFR Part 314.

For this Plan, PII means information that can identify a specific client, employee, or other person, alone or combined: a name together with a Social Security number, date of birth, driver's license or government ID number, financial account number, or similar identifier, in paper or electronic form. Information lawfully available to the public, like a listed business phone number, is not PII.

II. Purpose

`Rule anchor: 16 CFR 314.3(b), the program's three objectives`

The purpose of the Plan is to:

1. Ensure the security and confidentiality of the PII we hold.
2. Protect that information against anticipated threats and hazards to its security or integrity.
3. Guard against unauthorized access to or use of it that could result in substantial harm or inconvenience to any client, including identity theft or fraud.

III. Scope

The Plan covers every location and system where our firm's PII lives: our offices, our computers and devices, our tax and accounting software, our cloud services, and our paper files. In building and maintaining it, we identify reasonably foreseeable internal and external risks, assess how much damage each could do, evaluate the safeguards we already have, close the gaps we find, and monitor the result. The rule scales this duty to the firm: the program should fit our size and complexity, the nature and scope of our activities, and the sensitivity of the information at issue.

IV. Responsible officials

Rule anchor: 16 CFR 314.4(a), the Qualified Individual

The rule requires one named person to be responsible for overseeing, implementing, and enforcing the program. The rule calls this person the **Qualified Individual**; Publication 5708's sample calls the same role the **Data Security Coordinator (DSC)**. This template keeps the IRS's label. The two are the same seat.

Data Security Coordinator (DSC)

The DSC:

- Implements the Plan, including its daily operational protocols.
- Identifies where PII is stored (Attachment E) and treats those places as secured assets with restricted access.
- Maintains the authorized-access list (Attachment F) and updates it the day someone's access changes.
- Runs the annual security training and verifies every employee has completed it (Attachment D).
- Monitors compliance with the Plan and evaluates the security posture of the service providers in Attachment G.
- Reviews the Plan at least annually, and after any material change to the business or an incident, and logs the review in Attachment H.

DSC name and title: _____

Public Information Officer (PIO)

The PIO is the firm's single voice to the outside if an incident happens: clients, law enforcement follow-ups, the press if it comes to that. Routing every outward statement through one person prevents misunderstandings while the DSC works the technical side.

PIO name and title: _____

> YOUR FIRM DECIDES
>
> Who fills each seat. If your firm has two or more people, make the DSC and the PIO different people: one fixes, one speaks. In a solo practice both lines carry your own name, and naming yourself is not a formality: it is the rule's element (a), and it makes the review dates in Attachment H yours.

V. Risk assessment

Rule anchor: 16 CFR 314.4(b), the risk assessment the program is based on

Every safeguard in this Plan should trace back to a risk the firm actually has. List what you hold, where it lives, and what could realistically go wrong. The first row is a worked example to overwrite.

WHAT WE HOLD	WHERE IT LIVES	WHAT COULD GO WRONG	SAFEGUARD IN PLACE	PLANNED IMPROVEMENT
Example: client returns and source documents (SSNs, income, bank details)	Tax software, office server, cloud backup	Credentials phished; laptop stolen; backup exposed	MFA on every login; disk encryption; encrypted backup	Move archived years off the working server

> Note. Under 5,000 consumers: the rule sets aside the formal written risk assessment of 314.4(b)(1) (16 CFR 314.6). The assessment itself still has to happen, because the program must be based on one (314.4(b)). This grid is a sound way to do it at small-firm scale; larger firms should meet the written form of (b)(1), including criteria for how risks are evaluated and addressed.

VI. Inside the firm: information handling policies

PII collection and retention

Rule anchor: 16 CFR 314.4(c)(6), disposal and retention review

- We collect only the PII we need to do the work and meet our legal obligations.
- Access to PII is limited to employees whose job requires it (Attachment F).
- The DSC documents every place PII is stored: server, workstations, cloud services, filing cabinets (Attachment E).
- We destroy records when they are no longer needed for the work or required to be kept, per the retention periods and destruction methods in Attachment A.

YOUR FIRM DECIDES

Your retention period, in years, for client records, and your destruction methods. Set both in Attachment A. Tax records carry their own legal retention requirements; if you are unsure what applies to a record class, that is a question for a qualified professional.

Personnel accountability

Rule anchor: 16 CFR 314.4(e), training and personnel

- Every employee and contractor receives this Plan and signs the acknowledgment in Attachment D before accessing PII.
- New hires with PII access are screened before they start (reference checks at minimum; a background-check service if the firm chooses), and the firm records the step it used.
- The DSC trains all staff annually on this Plan and the rules of conduct in Attachment B, and keeps attendance records.
- Employees secure paper records and lock screens when away from their desks.
- Deliberate misuse of PII, or repeated disregard of this Plan, leads to discipline up to and including termination.
- On an employee's last day: logins disabled, remote and email access ended, keys and badges returned, and the change recorded in Attachment F.

PII disclosure

Rule anchor: 16 CFR 314.4(c)(1), access controls

- We do not disclose a client's PII to anyone without verifying who is asking and holding the client's written authorization, except where the law requires or permits the disclosure (for example, to tax authorities in the course of filing).
- Visitors do not enter areas where PII is kept unescorted.
- Records leave the office only when the work requires it, limited to the minimum needed, and come back promptly. Client files and devices are never left unattended in a car or another insecure place.
- The third parties we share PII with in the ordinary course of the work (tax software, e-filing, bookkeeping or payroll platforms, IT support) are listed in Attachment G and bound as Section VIII describes.

Reportable events

Related rule text: 16 CFR 314.4(h) and 314.4(j); see the note below

- Any suspected loss, theft, or unauthorized access to PII, however small it looks, is reported to the DSC the same day it is noticed.
- The DSC contains the problem, preserves evidence, and works through the incident procedures and notification contacts in Attachment C.
- After any incident, the DSC reviews what happened and updates this Plan if the incident exposed a gap (Attachment H).

> **YOUR FIRM DECIDES**
>
> Whether the firm carries cyber liability insurance or keeps counsel on retainer for incidents. Neither is required by the rule; both change your first phone calls. Record the decision, and the carrier or firm contact, in Attachment C's table.

> Note. Under 5,000 consumers: the written incident response plan of 314.4(h) is set aside (16 CFR 314.6). The notification duties are not. A reportable breach must still reach the FTC as soon as possible, within 30 days, once it involves 500 consumers (314.4(j)), and the IRS and state notification paths in Attachment C exist regardless of firm size. Keeping Attachment C filled in is how a small firm stays ready anyway.

VII. Outside the firm: technical safeguard policies

Network protection

`Rule anchor: 16 CFR 314.4(c)(8), monitoring and logging; 314.4(d), testing`

- A firewall separates our network from the internet, on the router, the computers, or both.
- Operating systems and software stay current: updates and security patches are applied promptly, and the DSC confirms patch status on a 30-day cycle.
- Reputable anti-virus and anti-malware protection runs and updates continuously on every machine that touches PII.
- Event logging is on where our systems support it, and the DSC reviews logs or account activity at intervals no longer than 90 days.

User access control

`Rule anchor: 16 CFR 314.4(c)(1) access; 314.4(c)(5) multi-factor authentication`

- Every user has a unique account. No shared logins, in the tax software or anywhere else.
- Passwords are strong (at least 8 characters mixing upper case, lower case, numbers, and symbols), unique per site, and changed on any sign of compromise; otherwise we refresh them on the cycle Publication 5708 suggests, once every 365 days.
- **Multi-factor authentication (MFA) is on for any individual accessing any information system.** Under the rule's definitions that reaches any system holding PII and any system connected to one that does. For a tax practice: tax software, email, cloud storage, remote access, the office network's admin logins, and the firm's IRS e-Services accounts.

The bolded sentence is the rule's own requirement, and it allows an alternative only one way: the Qualified Individual approves, in writing, access controls that are reasonably equivalent or more secure (16 CFR 314.4(c)(5)). If your firm ever uses that exception, file the written approval with this Plan.

> **YOUR FIRM DECIDES**
>
> Your MFA method (an authenticator app is stronger than text-message codes, and either is far stronger than none) and whether the firm uses a password manager. If it does, name it, require a strong master password, and turn MFA on for it too.

Electronic exchange and encryption of PII

Rule anchor: 16 CFR 314.4(c)(3), encryption in transit and at rest

- We do not send PII in a plain email, in the body or as an unprotected attachment.
- Client documents move through an encrypted portal, or as encrypted attachments with the password delivered separately (by phone or text, never in the same email).
- Customer information is encrypted at rest: full-disk encryption on computers and laptops, and encryption enabled on any USB or external drive that carries PII (BitLocker, FileVault, or equivalent).
- Where encrypting a particular system is genuinely infeasible, the rule permits alternative compensating controls only if the Qualified Individual reviews and approves them; that approval is filed with this Plan.

Wi-Fi access

- The office wireless network uses current strong encryption (WPA2 or WPA3) and a strong password.
- Guests never use the working network. If we offer guest Wi-Fi, it runs on a separate network or node.
- Every network device with a default password (router, printer, copier, smart devices) gets that password changed when it joins our network.

Remote access

Rule anchor: 16 CFR 314.4(c)(3) and (c)(5) applied to remote work

- Only remote-access tools the DSC has approved are used, and both the traffic and the login are encrypted (a VPN or an equivalent encrypted channel).
- Remote access requires MFA, every time.
- Publication 5708's sample disallows remote access outside business hours or when the office is unstaffed, to shrink the window an attacker can use.

> **YOUR FIRM DECIDES**
>
> Your after-hours rule. The IRS sample's default (no remote access outside business hours) is the cautious setting, and it is a poor fit for many firms in filing season. Decide what your firm actually does, write it here, and make the access log show it:
>
> _____

Connected devices and change management

Rule anchor: 16 CFR 314.4(c)(2) inventory; (c)(4) application security; (c)(7) change management

- A new device or service gets a quick security review by the DSC before it touches the network or PII, and an inventory line in Attachment E.
- AutoRun is disabled for USB and optical media on firm machines.
- New software is installed only with the DSC's approval, and outside applications that will touch PII get that security review before adoption (the 314.4(c)(4) duty; building software in-house is rare in a tax practice, and any firm that does follows secure development practices for it).
- Drives and devices leaving service are wiped or physically destroyed, per Attachment A.

Security training

`Rule anchor: 16 CFR 314.4(e), security awareness training`

- The DSC runs security training for all staff at least once a year: how we handle paper and electronic PII, the current phishing patterns aimed at tax practices, and what to do the moment something looks wrong.
- New hires are trained before they first touch PII.
- Everyone certifies attendance in writing (Attachment D), and the DSC keeps the records.

VIII. Service provider oversight

`Rule anchor: 16 CFR 314.4(f), overseeing service providers`

Publication 5708's sample touches vendors only in passing, but the rule gives them their own element, so this template adds one and says so. A tax practice runs on other people's software: tax prep, e-signature, portals, backup, email, sometimes an outside IT shop. Element (f) asks three things of the firm for each of them:

1. **Select** providers capable of protecting the PII they will touch. For mainstream tax and accounting platforms this is mostly reading their security page and knowing what you signed.
2. **Bind** them: the contract or terms of service must require safeguards. For large vendors this language already exists; the point is to know it is there.
3. **Reassess** them periodically, on a cycle you set, and when something changes or goes wrong.

The working list lives in Attachment G: every provider, what data it touches, and when you last looked.

> **YOUR FIRM DECIDES**
>
> Your reassessment cadence for Attachment G. Annually, alongside the Plan review in Attachment H, is a sound default for a small firm:
>
> _____

IX. Monitoring, testing, and annual review

`Rule anchor: 16 CFR 314.4(d) testing; (g) evaluate and adjust; (i) annual report`

- We check that our safeguards actually work: the DSC's 30-day patch check, the 90-day log review, and a yearly walk through this Plan against reality.
- We adjust the Plan when testing, an incident, or a business change says to (314.4(g)), and every adjustment lands in Attachment H.
- Once a year, the DSC writes a short status summary for the firm's owner: what changed, what was tested, what needs money or attention.

> Note. Under 5,000 consumers: the 314.4(d)(2) testing regime (continuous monitoring, or annual penetration testing plus vulnerability assessments at least every six months) and the formal written annual report under 314.4(i) are both set aside (16 CFR 314.6). The habit of testing what you rely on, and writing one page a year about it, is still what keeps a plan real. At or above 5,000, both duties apply in full, in those terms.

X. Implementation

Our firm has created this Written Information Security Plan in recognition of its duties under the Gramm-Leach-Bliley Act and the FTC Safeguards Rule (16 CFR Part 314). The Plan takes effect on the date below and remains in effect until it is replaced by a reviewed, dated successor. The undersigned have read it and accept responsibility for carrying it out.

X _____ Date: _____

Principal, partner, or owner · name and title: _____

X _____ Date: _____

Data Security Coordinator · name and title: _____

Attachment A: Record retention and disposal policy

`Rule anchor: 16 CFR 314.4(c)(6), secure disposal and retention review`

The rule's own timing formulation: customer information is disposed of securely no later than two years after the last date it is used in connection with serving that customer, unless it is still needed for business operations or another legitimate business purpose, a law or regulation requires keeping it, or targeted disposal is not reasonably feasible in the way the information is kept. The same subsection asks the firm to periodically review its retention policy so it is not holding data it no longer needs.

We retain client records for: _____ years after the engagement ends, unless a law or regulation requires longer.

When a record's retention period ends, we destroy it:

- **Paper**: cross-cut shredding or incineration. Never whole pages in the trash.
- **Electronic**: deletion plus overwriting, or full-disk reformatting; drives leaving service are wiped with a disk utility or physically destroyed.

> Note. Retention floors for tax records come from tax law, not from this Plan; when a record class has its own required period, that period wins. Setting the number for your firm is a judgment call worth confirming with a qualified professional.

Attachment B: Rules of behavior and conduct

Every employee and contractor with access to PII agrees to these working rules:

- Never share your login or MFA codes with anyone, inside the firm or out.
- Lock your screen when you step away; secure paper files before you leave.
- Treat unexpected attachments and links as hostile until verified, especially during filing season.
- Verify any request to change bank details, e-file credentials, or client contact information through a second channel you initiate.
- Requests to "verify" the firm's EFIN, PTIN, or e-Services login go to the DSC before anyone replies. The IRS warns that criminals impersonate the IRS and software vendors to harvest exactly these credentials.
- No PII on personal devices or personal cloud accounts unless the DSC has approved the device and it is encrypted.
- No PII in text messages or consumer chat apps.
- Report anything that looks off to the DSC the same day. Reporting a near miss is a good outcome, not a confession.

Attachment C: Security incident procedures and notification contacts

Related rule text: 16 CFR 314.4(h) (set aside under 5,000 consumers) and 314.4(j)

If PII may have been lost, stolen, or accessed without authorization, the DSC works this sequence:

1. **Contain it.** Disconnect the affected machine from the network; disable compromised accounts; change the passwords that matter. Do not wipe or reinstall anything yet.
2. **Preserve the evidence.** Note what happened, when it was noticed, and what was touched. Keep logs and the affected hardware as they are.
3. **Call the IRS Stakeholder Liaison quickly.** The IRS's own guidance stresses that speed is critical: reported fast, the IRS can move to block fraudulent returns filed with your clients' information.
4. **Bring in the professionals you decided on** in Section VI: your insurer's breach hotline if you carry cyber coverage, counsel if you keep one, or an IT security firm.
5. **Count who is affected.** The FTC and state duties below turn on numbers and residency, so an honest count comes early.
6. **Notify the rest of the table** as each duty triggers, and let the PIO handle every outward statement, including to clients.

WHO	WHEN	HOW
IRS Stakeholder Liaison	Quickly, on discovery of a data theft	irs.gov: "Data theft information for tax professionals". Your local liaison contact: _____
FTC (Safeguards Rule notification event)	As soon as possible, and no later than 30 days after discovery, if unencrypted information of 500 or more consumers is involved (16 CFR 314.4(j))	The FTC's Safeguards Rule Security Event Reporting Form, on ftc.gov. The FTC notes a submitted report may be made public.
State tax agencies	Per each affected state's process	Each state where affected clients file. Your primary state contact: _____
State Attorneys General	Per each state's breach notification law; deadlines and thresholds vary by state	Each state where affected clients live. Where your clients concentrate: _____
Local police / FBI	Promptly for theft or intrusion; the IRS also points tax professionals to the FBI	Local department; FBI field office or ic3.gov. Local numbers: _____
Tax software vendor	Promptly; vendors can watch for misuse of your credentials	Your vendor's security contact: _____
Cyber insurer or counsel	Per your policy or engagement; many policies require notice before other steps	Carrier or firm, policy number, hotline: _____

WHO	WHEN	HOW
Affected clients	Timing coordinated with law enforcement and any state-law deadline	Written notice drafted by the PIO; state law may prescribe content. Credit bureaus may also need notice under state law.

Prepared by Safeguards Monitor from IRS “Data theft information for tax professionals”, the FTC Safeguards Rule Security Event Reporting Form page, and 16 CFR 314.4(j), each checked July 17, 2026. Fill in your local contacts now, not during an incident.

> Note. Under 5,000 consumers: the rule sets aside the formal written incident response plan (314.4(h)). It does not set aside any notification in this table. The FTC report (as soon as possible, within 30 days, at 500 or more consumers), the IRS path, and state breach laws all stand regardless of firm size.

Attachment D: Employee and contractor acknowledgment

I acknowledge that I have received and read the firm’s Written Information Security Plan, including the rules of behavior in Attachment B. I understand my responsibilities for protecting client information, I agree to follow the Plan, and I understand that violating it can lead to discipline up to and including termination of my employment or engagement. I agree to complete the firm’s security training when it is scheduled.

X _____ Date: _____

Employee or contractor · name and title: _____

X _____ Date: _____

For the firm (DSC or principal) · name and title: _____

Attachment E: Hardware and systems inventory

Rule anchor: 16 CFR 314.4(c)(2), knowing what you have

List every device and service where PII lives or passes: computers, laptops, phones used for work, the server, routers, printers with storage, external drives, and cloud services (tax software, portal, backup, email). Cloud services belong on this list; an inventory that stops at physical hardware misses where most of a modern firm’s PII actually sits.

ITEM OR SERVICE	LOCATION OR PROVIDER	PRINCIPAL USER	HOLDS PII?	IN SERVICE SINCE	LAST CHECKED
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

ITEM OR SERVICE	LOCATION OR PROVIDER	PRINCIPAL USER	HOLDS PII?	IN SERVICE SINCE	LAST CHECKED
_____	_____	_____	_____	_____	_____
_____	_____	_____	_____	_____	_____

Attachment F: Authorized access list

Rule anchor: 16 CFR 314.4(c)(1), limiting access to what the work needs

Who can access PII, what they can reach, and when that changed. When someone's access changes, close the old line and open a new one; the history is the point.

NAME	ROLE	WHAT THEY CAN ACCESS	GRANTED	ENDED
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

Attachment G: Service provider list

Rule anchor: 16 CFR 314.4(f), overseeing service providers

PROVIDER	SERVICE	DATA IT TOUCHES	CONTRACT REQUIRES SAFEGUARDS?	LAST ASSESSED
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

Attachment H: Record of review and changes

Rule anchor: 16 CFR 314.4(g), evaluating and adjusting the program

Review this Plan at least once a year, and after any material change or incident. A dated line here is what separates a living plan from a form that was filled in once.

DATE	WHAT WAS REVIEWED OR CHANGED	BY
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Sources and further reading

Every regulatory reference in this template was checked against the primary source on July 17, 2026.

IRS Publication 5708, "Creating a Written Information Security Plan" (Rev. 8-2024)

The IRS template this document is adapted from.
https://www.irs.gov/pub/irs-pdf/p5708.pdf

IRS Publication 4557, "Safeguarding Taxpayer Data" (Rev. 6-2024)

The IRS's companion guide, with its own checklist.
https://www.irs.gov/pub/irs-pdf/p4557.pdf

16 CFR Part 314, the FTC Safeguards Rule (eCFR, current text)

The rule itself. Sections 314.3, 314.4, and 314.6 are the ones this template anchors to.
https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

FTC, "FTC Safeguards Rule: What Your Business Needs to Know" (updated December 2024)

The FTC's plain-language compliance guide; it names tax preparation firms as covered.
https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

FTC, Safeguards Rule Security Event Reporting Form

Where the 30-day, 500-consumer breach report is filed.
https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act/safeguards-rule-form

IRS, "Data theft information for tax professionals"

The IRS's incident path, including the Stakeholder Liaison contact.
https://www.irs.gov/individuals/data-theft-information-for-tax-professionals

IRS Form W-12 (Rev. October 2025)

The PTIN application and renewal form; Line 11 is the data-security awareness attestation.
https://www.irs.gov/pub/irs-pdf/fw12.pdf

About this document

This template is published by **Safeguards Monitor** (safeguardsmonitor.com), an independent publication on Written Information Security Plan and FTC Safeguards Rule compliance for US tax professionals. It is free, it is not gated behind an email address, and the current version always lives at safeguardsmonitor.com/wisp-template. This is version 1.0, July 2026. If you spot an error, write to hello@safeguardsmonitor.com; we publish dated corrections.

> **DISCLAIMER**
>
> This template is educational, adapted from IRS Publication 5708. It is general information, not legal advice for your specific situation, and completing it does not by itself make your firm compliant. For advice on your situation, consult a qualified professional.