Written Information Security Plan

`[FIRM NAME]` Adopted: `[DATE]` · Last reviewed: `[DATE]` · Version: 1.0

How to use this document

This is a working template for a US tax, accounting or bookkeeping practice with roughly 3 to 25 people. It follows the structure of the FTC Safeguards Rule (16 CFR Part 314) and IRS Publication 5708.

Three rules for filling it in:

1. **Replace every `[BRACKETED]` field.** A plan with brackets left in it is evidence that nobody read it.
2. **Delete what does not apply to you.** A shorter plan that is true beats a longer one that is aspirational. If you have no remote staff, say so and cut the remote-access section.
3. **Write what you actually do, then fix what you find.** The gap between the two is the useful part of this exercise.

Sections marked `[EXEMPT UNDER 5,000]` are not required if your firm maintains information on fewer than 5,000 consumers (16 CFR 314.6). Most small practices qualify. Keeping them anyway is good practice, and they are short.

> This template is general information, not legal advice. Every requirement below cites the exact section it comes from, so you can check any statement against the regulation yourself rather than taking this document's word for it. The sources are listed on the last page, all of them free and online.
>
> The IRS publishes its own sample plan inside Publication 5708. This template is a companion to it, not a replacement: it adds the inventories, logs and vendor questions that the sample leaves to you.

---

1. Purpose and scope

This plan describes how `[FIRM NAME]` protects the information it holds about its clients, and how the firm meets its obligations under the FTC Safeguards Rule (16 CFR Part 314), issued under the Gramm-Leach-Bliley Act.

Scope. This plan covers all customer information held by the firm in any form — electronic, paper, or otherwise — and everyone who handles it: owners, employees, contractors, and temporary seasonal staff.

Customer information means any record containing non-public personal information about a client, whether in paper, electronic or other form, that is handled by or on behalf of the firm.

Objectives, as stated in the rule:

- ensure the security and confidentiality of customer information

- protect against anticipated threats or hazards to its security or integrity
- protect against unauthorised access that could result in substantial harm or inconvenience to any client

---

2. Firm information

FIELD	ENTRY
Legal name	`[FIRM NAME]`
Trading name	`[DBA, IF ANY]`
Address	`[ADDRESS]`
EFIN / PTIN holder(s)	`[LIST]`
Number of staff with access to client data	`[N]`
Approximate number of clients	`[N]`
Fewer than 5,000 consumers?	`[YES / NO]`
Plan owner	`[NAME]`

---

3. Qualified Individual (16 CFR 314.4(a))

The firm designates **`[NAME, TITLE]`** as the Qualified Individual responsible for overseeing, implementing and enforcing this information security program.

This person:

- maintains this document and the inventories in the appendices
- approves access for new staff and removes it when someone leaves
- reviews vendors that handle client data
- decides what happens during a security incident
- reports to `[OWNER / MANAGING PARTNER]` on the state of the program

If the role is filled by an outside provider, the firm retains responsibility and designates **`[NAME]`** internally to direct that provider.

Backup. If the Qualified Individual is unavailable, **`[NAME]`** acts in their place.

---

4. Information inventory (16 CFR 314.4(c)(2))

You cannot protect what you have not listed. Complete Appendix A before continuing — for most firms this is the single most valuable part of the exercise, and almost nobody has it.

The firm maintains an inventory of:

- every system, application and device that stores or transmits client data
- where each one physically stores that data
- who has access to it
- what happens to the data when the firm stops using that system

The inventory is reviewed at least annually and whenever the firm adopts or retires a system.

---

5. Risk assessment (16 CFR 314.4(b)) `[EXEMPT UNDER 5,000 — written form not required]`

The firm considers, at least annually:

THREAT	LIKELIHOOD	IMPACT	CURRENT CONTROL
Phishing email leading to credential theft	`[H/M/L]`	`[H/M/L]`	`[CONTROL]`
Lost or stolen laptop or phone	`[H/M/L]`	`[H/M/L]`	`[CONTROL]`
Ransomware on the office network	`[H/M/L]`	`[H/M/L]`	`[CONTROL]`
Employee or contractor misuse	`[H/M/L]`	`[H/M/L]`	`[CONTROL]`
Vendor or cloud provider breach	`[H/M/L]`	`[H/M/L]`	`[CONTROL]`
Paper files left accessible	`[H/M/L]`	`[H/M/L]`	`[CONTROL]`
Client data emailed unencrypted	`[H/M/L]`	`[H/M/L]`	`[CONTROL]`

Add rows for anything specific to your practice. Where a control is missing, say so and record a target date rather than leaving the cell optimistic.

---

6. Safeguards (16 CFR 314.4(c))

6.1 Access controls

- Access to client data is granted on a least-privilege basis: each person can reach only what their work requires.

- Access is reviewed `[QUARTERLY / ANNUALLY]` by the Qualified Individual.
- Access is removed **the same day** a person leaves the firm or changes role. See the off-boarding checklist in Appendix D.
- Shared logins are not used. Each person has their own account. `[IF A SHARED ACCOUNT EXISTS, NAME IT AND STATE THE PLAN TO ELIMINATE IT.]`

6.2 Encryption

- Client data is encrypted in transit and at rest.
- Full-disk encryption is enabled on every laptop and desktop that touches client data: `[LIST DEVICES OR "all firm devices"]`.
- Mobile devices with firm email are encrypted and screen-locked.
- Where encryption is infeasible for a particular system, the Qualified Individual has approved the compensating control described here: `[DESCRIBE OR DELETE]`.

6.3 Multi-factor authentication (16 CFR 314.4(c)(5))

MFA is required for every account that can reach client data — not only email.

SYSTEM	MFA ENABLED	METHOD
Email	`[YES/NO]`	`[APP / KEY / SMS]`
Tax preparation software	`[YES/NO]`	`[METHOD]`
Accounting / bookkeeping software	`[YES/NO]`	`[METHOD]`
Document storage	`[YES/NO]`	`[METHOD]`
Remote access / VPN	`[YES/NO]`	`[METHOD]`
Payroll or banking portals	`[YES/NO]`	`[METHOD]`

SMS is weaker than an authenticator app or a hardware key. Use it only where nothing better is offered.

6.4 Data retention and disposal (16 CFR 314.4(c)(6))

- Client information is disposed of **no later than two years** after the last date it was used to provide a service, unless retention is required by law or necessary for a legitimate business purpose.
- The firm's retention period is `[N]` years, based on `[REASON: e.g. IRS record retention guidance, state requirement, engagement terms]`.
- Paper is shredded on site / by `[VENDOR]`. Electronic media is wiped or destroyed before disposal, never simply thrown out or resold.
- Disposal is logged in Appendix E.

6.5 Change management (16 CFR 314.4(c)(7))

Before adopting new software, moving to a new provider, or changing how client data is stored, the Qualified Individual records the change, what data it touches, and what was checked. Log it in Appendix C.

6.6 Monitoring of user activity (16 CFR 314.4(c)(8))

The firm `[ENABLES AUDIT LOGGING IN / RELIES ON THE PROVIDER'S LOGS FOR]` the systems listed in Appendix A. Logs are reviewed `[MONTHLY / AFTER ANY INCIDENT]` by `[NAME]`.

6.7 Physical security

- The office is locked outside working hours; client files are not left visible.
- Paper files are stored in `[LOCATION]`, locked when unattended.
- Visitors do not have unescorted access to areas where client data is kept.

6.8 Remote work and travel

`[DELETE THIS SECTION IF NOBODY WORKS REMOTELY.]`

- Remote access is through `[VPN / REMOTE DESKTOP / CLOUD APPLICATIONS ONLY]`.
- Client data is not stored on personal devices.
- Public Wi-Fi is used only with the VPN active.

---

7. Testing and monitoring (16 CFR 314.4(d)) `[EXEMPT UNDER 5,000 — continuous monitoring / annual penetration testing not required]`

The firm verifies annually that:

- MFA is still on for every system in the table above
- former staff no longer have access to anything
- backups restore successfully — **tested**, not assumed, on `[DATE]`
- devices are still encrypted and patched

Date of last verification: `[DATE]`. Performed by: `[NAME]`.

---

8. Security awareness training (16 CFR 314.4(e))

Everyone with access to client data receives security training:

- at hire, before receiving access
- at least annually thereafter
- before each filing season, covering current phishing patterns

Training covers: recognising phishing and pretexting, handling client data, password and MFA practice, reporting an incident, and clean-desk habits.

Training is recorded in Appendix B. **The record is the part an examiner asks for.** Training that happened but was not written down did not happen.

---

9. Service provider oversight (16 CFR 314.4(f))

The firm uses outside providers that handle or can reach client data. For each one (Appendix C) the firm:

- selects providers capable of maintaining appropriate safeguards
- requires by contract that they do so
- reviews them at least annually, or when the service changes materially

Questions asked of each provider:

1. Where is our data stored, and under whose jurisdiction?
2. Who at your company can read our clients' documents?
3. Is data encrypted at rest and in transit?
4. Do you offer MFA, and do you support hardware keys?
5. How do we export everything if we leave, and how long does it take?
6. Will you notify us of a breach, and within how long?
7. What certifications or audits do you hold, if any?

---

10. Evaluation and adjustment (16 CFR 314.4(g))

This plan is reviewed and updated:

- at least annually
- after any security incident
- when the firm changes software, providers, premises or staffing materially
- when the rules change

Revision history is kept on the last page.

---

11. Incident response plan (16 CFR 314.4(h)) `[EXEMPT UNDER 5,000 — written plan not required]`

Recommended regardless: during an incident nobody invents a good procedure.

Step 1 — Contain. Disconnect the affected device from the network. Do not wipe or "clean" it; it is evidence. Change passwords for affected accounts from a different, known-good device.

Step 2 — Notify internally. Tell the Qualified Individual immediately. Contact: `[NAME, PHONE]`.

Step 3 — Assess. What data, whose data, how many people, what was taken or encrypted, and is it still happening.

Step 4 — Report externally. As applicable:

WHO	WHEN	CONTACT
IRS Stakeholder Liaison	as soon as possible after a data theft	`[LOCAL CONTACT]`
State tax agency / FTA	promptly	`[CONTACT]`
FTC — breaches affecting 500+ consumers (16 CFR 314.4(j))	**as soon as possible, no later than 30 days after discovery**	ftc.gov
State attorney general	per state breach law	`[CONTACT]`
Clients affected	per state law and engagement terms	—
Cyber insurance carrier	immediately; late notice can void cover	`[POLICY NUMBER]`
Local FBI field office / IC3	for ransomware and theft	ic3.gov

Step 5 — Recover. Restore from backup, verify integrity, reset all credentials, confirm the entry point is closed.

Step 6 — Write it down. What happened, when it was found, what was done, and what changes to this plan follow. Log in Appendix F.

---

12. Reporting to management (16 CFR 314.4(i)) `[EXEMPT UNDER 5,000]`

The Qualified Individual reports at least annually to `[OWNER / MANAGING PARTNER]` on the overall status of the program, risks identified, incidents, and recommended changes. Date of last report: `[DATE]`.

---

13. IRS "Security Six" checklist

The IRS's short list, published for tax professionals. If any of these is missing, this plan is not credible.

CONTROL	IN PLACE	DETAIL
Anti-virus software	`[YES/NO]`	`[PRODUCT]`
Firewall	`[YES/NO]`	`[PRODUCT / ROUTER]`
Multi-factor authentication	`[YES/NO]`	see 6.3
Backup of client data	`[YES/NO]`	`[WHERE, HOW OFTEN, LAST RESTORE TEST]`
Drive encryption	`[YES/NO]`	see 6.2
VPN for remote access	`[YES/NO]`	`[PRODUCT]`

14. Adoption

This plan is adopted by the firm and applies to everyone with access to client information.

Qualified Individual	`[NAME]` · Signature: _ · ***Date:*** ___
Owner / Managing Partner	`[NAME]` · Signature: _ · ***Date:*** ___

Acknowledgement. Every person with access signs below to confirm they have read this plan.

NAME	ROLE	SIGNATURE	DATE

Appendix A — System and data inventory

SYSTEM / APPLICATION	WHAT CLIENT DATA IT HOLDS	WHERE DATA IS STORED	WHO HAS ACCESS	MFA

Appendix B — Training log

DATE	TOPIC	ATTENDEES	DELIVERED BY

Appendix C — Service providers

PROVIDER	SERVICE	DATA IT CAN REACH	LAST REVIEWED	CONTRACT REQUIRES SAFEGUARDS

Appendix D — Off-boarding checklist

- [ ] Email account disabled
- [ ] Tax and accounting software access removed
- [ ] Document storage access removed
- [ ] VPN / remote access revoked
- [ ] Shared credentials rotated
- [ ] Firm devices returned and wiped
- [ ] Keys and building access returned
- [ ] Completed by `[NAME]` on `[DATE]`

Appendix E — Disposal log

DATE	WHAT WAS DISPOSED OF	METHOD	BY WHOM

Appendix F — Incident log

DATE DISCOVERED	WHAT HAPPENED	DATA INVOLVED	ACTIONS TAKEN	REPORTED TO	CLOSED

Revision history

VERSION	DATE	CHANGED BY	WHAT CHANGED
1.0	`[DATE]`	`[NAME]`	Initial adoption

Sources

Every statement in this template comes from one of these. All are free to read.

CLAIM	SOURCE
Tax and accounting professionals are financial institutions regardless of size	IRS Publication 5708 (Rev. 8-2024), "Requirements"
The nine program elements, paragraphs (a) to (i)	16 CFR 314.4
Disposal of customer information no later than two years after last use	16 CFR 314.4(c)(6)
Continuous monitoring or periodic penetration testing and vulnerability assessments	16 CFR 314.4(d)(2)
Notify the FTC of an event involving 500+ consumers, no later than 30 days after discovery	16 CFR 314.4(j)(1)
Firms with fewer than 5,000 consumers are exempt from 314.4(b)(1), (d)(2), (h) and (i)	16 CFR 314.6
The "Security Six"	IRS Security Summit / Publication 4557
PTIN holders attest to the WISP requirement	Form W-12 (Rev. 10-2025), line 11

Line 11 of Form W-12 reads: *"I am aware that paid tax return preparers are required by law to create and maintain a written information security plan that provides data and system security protections for all taxpayer information."* You check that box every renewal.

Citations verified against the sources on 8 September 2026. Regulations change — check the current text before relying on any of this.
