



2026

Written Information Security Plan

Built following IRS Publication 4557

Northgate Tax & Advisory, PC

CA

WISP Version: 2026 | Effective: January 1, 2026

Generated by CPA Hub | 2026 Annual Security Plan

SAMPLE · Northgate Tax & Advisory is a made-up firm. Every person and device in this plan is invented, and every vendor except CPA Hub.

Program Summary

Northgate Tax & Advisory, PC — 16 CFR Part 314, FTC Safeguards Rule

The state of this firm's program as of 9/15/2026. Every claim below is evidenced in the pages and attachments that follow.

HIGHEST-PRIORITY OPEN FINDING

1 device holds client data and is not encrypted — starting with Front-desk scanner PC.

OK §314.4(a)	Qualified Individual Morgan Ellis, Managing Partner — designated January 6, 2025 <i>Readiness check passed August 20, 2026 — 9 of 10 on this firm's own program.</i>
OK §314.4(b)	Risk assessment February 11, 2026 — overall risk moderate
OK §314.4(c)(1)	What we hold Social Security Numbers, Financial Records, Tax Returns, Bank Account Info — across 7 of 7 devices
OPEN §314.4(c)(3)	Encryption at rest 6 of 7 encrypted <i>Not encrypted: Front-desk scanner PC</i> They ask: Is customer information encrypted at rest?
OK §314.4(c)(6)	Retention & disposal Tax returns 7y, client records 7y — electronic: cryptographic erase
OPEN §314.4(f)	Service providers 6 registered, 5 with a written agreement They ask: Who are your service providers and how do you oversee them?
OK §314.4(e)	Security awareness training 6 of 6 passed, most recent March 6, 2026
OK §314.4(h)	Incidents 1 in 2026, all resolved
OK §314.4(i)	Annual review January 27, 2026
OK 16 CFR 314.3	The written plan 8 of 8 required sections complete

Open items

CRITICAL §314.4(c)(3) 1 device holds client data and is not encrypted — starting with Front-desk scanner PC.

IMPORTANT §314.4(f) 1 provider has no written agreement on file.

About This Document

Purpose

This Written Information Security Plan (WISP) is a federally mandated document required by the FTC Safeguards Rule (16 CFR 314) for all professional tax preparers. It establishes your firm's policies and procedures for protecting client personally identifiable information (PII), including Social Security numbers, financial records, and tax return data.

This document serves three critical functions:

1. **Compliance** - Puts in writing the program 16 CFR 314.4 requires the firm to keep
2. **Protection** - Provides a framework for safeguarding client information
3. **Response** - Guides your team through security incidents when they occur

How to Use This Document

Policy Sections

Each section contains specific policies tailored to your firm. Review these with all employees and ensure everyone understands their responsibilities.

Checklists []

Throughout this document, you'll find checkbox items. These are actionable checklists for specific procedures. When performing tasks like incident response, data destruction, or employee offboarding, use these as step-by-step guides to ensure nothing is missed.

Document Control

Your WISP is a living document: IRS Publication 5708 recommends a review at least annually, and 16 CFR 314.4(g) requires adjusting it when operations change. Update it when:

- Your firm's size or operations change
- You adopt new technology or systems
- A security incident reveals gaps
- Regulations change

Required Actions

1. **READ** - All employees must read and understand this document
2. **SIGN** - Employees should acknowledge receipt and understanding
3. **STORE** - Keep copies both on-site and in secure cloud/offsite storage
4. **REVIEW** - Conduct annual reviews (suggested: each May after tax season)
5. **UPDATE** - Revise as your firm and technology evolve

Questions? Contact your Data Security Coordinator listed on the cover page.

Designated Security Coordinator

Northgate designates Morgan Ellis, Managing Partner, as its Data Security Coordinator under 16 CFR 314.4(a). The Coordinator implements, maintains and enforces this plan, oversees the annual risk assessment, staff training, service-provider oversight and incident response, and reports to the partners at least once a year.

SAMPLE

Risk Assessment

The firm completes a written risk assessment every year, identifying reasonably foreseeable internal and external risks to the confidentiality, integrity and availability of client information - staff access, remote work, e-mail, portable media, physical security and service providers. Each risk is rated for likelihood and impact and mapped to a control.

SAMPLE

Multi-Factor Authentication & Access Policy

Every system that stores or transmits client information requires multi-factor authentication. Access is least-privilege, reviewed quarterly and removed the day someone leaves. Shared accounts are not permitted; each person has a unique login.

SAMPLE

Encryption Policy

Client information is encrypted at rest and in transit (TLS 1.2 or later). Every laptop, workstation and server that holds client information uses full-disk encryption. Client documents are exchanged through the secure portal, never as unencrypted e-mail attachments.

SAMPLE

Incident Response Plan

When a security event is suspected, the Coordinator contains it, assesses its scope, preserves evidence, and - where client information may have been acquired - notifies affected clients, the IRS Stakeholder Liaison, state authorities as required, and the FTC within 30 days of discovery where 500 or more consumers are involved. Every incident is logged and reviewed.

SAMPLE

Employee Security Training

Everyone with access to client information completes security awareness training when hired and every year after, covering phishing, passwords and MFA, handling client PII and reporting incidents. Completion is recorded and kept.

SAMPLE

Third-Party Vendor Management

Service providers with access to client information are selected for their ability to protect it, bound by a written agreement requiring safeguards, and reviewed at least annually. The firm keeps a current register of every such provider.

SAMPLE

Data Retention & Disposal

Client records are kept seven years and then destroyed: cross-cut shredding for paper, cryptographic erasure for electronic media. Information no longer needed for a business purpose is disposed of within two years of last use.

SAMPLE

CIRCULAR 230 · IRS OPR ISSUE NUMBER 2026-19

Responsible AI Use - 2026

Northgate Tax & Advisory, PC

Source: IRS Office of Professional Responsibility, Issue Number 2026-19, "Introductory Guidelines for Responsible AI Use in Federal Tax Practice" (June 24, 2026). Introductory guidelines. They create no new rule; each point rests on an existing Circular 230 duty that OPR enforces.

This section is part of the firm's written plan but is not an FTC Safeguards Rule requirement, and it does not count toward any FTC finding in this document.

Where the firm stands

Staff trained on AI: 5 of 6 passed the AI module

OK	Written AI policy Written and saved in this year's WISP	31 CFR 10.36
OK	Human review of AI output Every AI output is reviewed by a person before it reaches a client or the IRS	31 CFR 10.22, 10.37
OK	AI tools listed 3 AI tools in the service-provider register	31 CFR 10.36
OK	Client data in AI tools 3 approved for client data, 0 not	IRC 6713, 7216(a)
NOT RECORDED	Vendor training on firm data NOT RECORDED for 1 approved tool	31 CFR 10.36; IRC 7216(a)
OPEN	Staff trained on AI 5 of 6 passed the AI module	31 CFR 10.35, 10.36
OK	Record of AI use The firm keeps a record of where AI was used and how it was checked CPA Hub records its own AI use automatically - see the record below.	31 CFR 10.36

5 of 7 answered and current, 1 open, 1 not recorded.

The firm's AI policy

Northgate follows IRS Office of Professional Responsibility Issue Number 2026-19, "Introductory Guidelines for Responsible AI Use in Federal Tax Practice" (June 24, 2026). Those guidelines create no new rule; each point below rests on an existing Circular 230 duty.

Approved tools. Only AI tools the Data Security Coordinator has approved are used for firm work. Each is listed, with its decisions, in the firm's service-provider register (31 CFR 10.36). Personal and free AI accounts are not used for firm work.

Client data. Client information goes only into AI tools approved for it, under business terms that protect confidentiality, and never into a public or personal account (IRC 6713, 7216(a)).

Human review. Everything an AI tool produces is a draft. Before it reaches a client or the IRS, a preparer checks the facts, the calculations and every citation (31 CFR 10.22). Written advice never rests on AI output that has not been independently verified (31 CFR 10.37).

Fees. Bills reflect the time the work actually took; the firm does not charge for manual time an AI tool replaced (31 CFR 10.27(a)).

Training. Everyone who uses AI completes the firm's AI module before using it and every year after (31 CFR 10.35, 10.36).

Records. Where AI was used on a return and how it was checked is noted in the workpapers. CPA Hub records its own AI use automatically.

Errors and disclosures. A wrong AI output that reached a client, or client information entered into an unapproved tool, is reported to the Data Security Coordinator the same day, corrected, and handled under the incident response plan where needed.

This policy is reviewed every year with the rest of the plan.

AI tools in the service-provider register

CPA Hub

Approved for client data · Does not train on our data · Written agreement on file

Email host

Approved for client data · NOT RECORDED whether it trains on our data · Written agreement on file

Tax software provider

Approved for client data · Does not train on our data · Written agreement on file

Record of AI use in CPA Hub - 2026

Every AI call CPA Hub made for this firm, logged automatically when it happened. AI tools used outside CPA Hub keep no record here.

No AI use recorded in CPA Hub for 2026.

2026 WISP Acknowledgment & Approval

This 2026 Written Information Security Plan has been reviewed and approved for implementation at Northgate Tax & Advisory, PC.

WISP Version: 2026

This document covers the 2026 compliance year. IRS Publication 5708 recommends reviewing it at least annually, and 16 CFR 314.4(g) requires adjusting it when your operations change.

Designated Security Coordinator:

Signature

Date

Firm Principal / Owner:

Signature

Date

Annual Review Schedule

IRS Publication 5708 recommends reviewing and updating this WISP at least annually. The FTC Safeguards Rule requires adjusting it whenever there is a material change to your operations or business arrangements (16 CFR 314.4(g)).

Next Review Due: January 1, 2027

Attachment A — Designated Officials

16 CFR §314.4(a) requires the firm to designate a qualified individual responsible for overseeing and implementing this information security program.

Data Security Coordinator

Name	Morgan Ellis
Title	Managing Partner
Email	morgan.ellis@example.com
Phone	Not recorded
Date designated	1/6/2025

Qualifications

CPA. Oversees the firm technology program; completed security awareness and incident response training.

SAMPLE

Attachment B — Record Retention Schedule

16 CFR §314.4(c)(6) — retention periods and secure disposal methods adopted by the firm.

Tax returns & supporting documents	7 years
Client records	7 years
Client correspondence	3 years
Employee records	4 years after termination
Financial records	7 years
WISP & security documentation	Retained for the life of the program plus three years.

Disposal methods

Paper records	cross-cut shredding
Electronic records	cryptographic erase

SAMPLE

Attachment C — Hardware Inventory

16 CFR §314.4(c) — equipment that stores or processes customer information. §314.4(c)(3) requires that information to be encrypted at rest.

File server

Type: server · Location: Main office

Client data: Social Security Numbers, Financial Records, Tax Returns, Bank Account Info

Encryption: Encrypted (method not recorded)

Front-desk scanner PC

Type: desktop · Location: Main office · Principal user: Tessa Barlow

Client data: Social Security Numbers, Tax Returns

Encryption: NOT ENCRYPTED

Office manager workstation

Type: desktop · Location: Main office · Principal user: Kenji Morrow

Client data: Social Security Numbers, Tax Returns, Bank Account Info

Encryption: Encrypted (method not recorded)

Partner laptop (Ellis)

Type: laptop · Location: Main office · Principal user: Morgan Ellis

Client data: Social Security Numbers, Financial Records, Tax Returns

Encryption: Encrypted (method not recorded)

Preparer laptop 1

Type: laptop · Location: Main office · Principal user: Avery Lindqvist

Client data: Social Security Numbers, Financial Records, Tax Returns

Encryption: Encrypted (method not recorded)

Preparer laptop 2

Type: laptop · Location: Main office · Principal user: Rafael Ortiz

Client data: Social Security Numbers, Financial Records, Tax Returns

Encryption: Encrypted (method not recorded)

Preparer laptop 3

Type: laptop · Location: Main office · Principal user: Joanna Pike

Client data: Social Security Numbers, Financial Records, Tax Returns

Encryption: Encrypted (method not recorded)

Devices in service: 7

Recording client data: 7

1 device holds client data and is not encrypted — §314.4(c)(3) exception.

Attachment D — Risk Register

16 CFR §314.4(b) — reasonably foreseeable risks identified by the firm, and the safeguards adopted to address them. Complements the scored risk assessment.

Return information e-mailed to an advisory firm outside the platform

Type: external · Likelihood: medium · Impact: high · Status: open · Identified: 4/18/2026

Mitigation: All advisory disclosure routed through consented channels.

SAMPLE