WISP template

United States edition

Grouped by the elements of 16 CFR 314.4. Where the rule relieves a firm holding information on fewer than 5,000 consumers, the note says so. Replace the bracketed text with your firm's details.

SCOPE AND OBJECTIVES

- [ ] What the plan covers, including paper records, devices and cloud systems
- [ ] The kinds of customer information the firm holds, and where each is kept
  Publication 5708's outline starts here: list the information you handle before you assess the risks to it.
- [ ] The date the plan takes effect, and who in the firm adopted it
- [ ] How often the plan is reviewed, and the date of the last review

QUALIFIED INDIVIDUAL — §314.4(A)

- [ ] The name of the Qualified Individual who oversees and enforces the plan
- [ ] If that person is outside the firm, the senior person who directs and oversees them
  The Qualified Individual may work for a service provider, but the firm keeps responsibility for compliance, and the provider must maintain a security program that protects the firm.
- [ ] Authorized users, their access levels and responsibilities
- [ ] The date each user's access was granted, and the date it ended
  Publication 5708's Attachment F is a table for exactly this: name, role, duties, access level, and the dates access was granted and terminated.

RISK ASSESSMENT — §314.4(B)

- [ ] The written risk assessment, with the criteria used to rate each risk
  A firm with customer information on fewer than 5,000 consumers is exempt from the requirement that the risk assessment be written (§314.6). It still has to assess the risks.
- [ ] How the confidentiality, integrity and availability of systems and data were assessed
- [ ] How each identified risk will be mitigated or accepted
- [ ] When the next risk assessment is due

SAFEGUARDS — §314.4(C)

- [ ] Access controls, limiting each user to the customer information their duties need
- [ ] An inventory of the data, people, devices, systems and facilities the firm relies on
- [ ] Encryption of customer information in transit over external networks and at rest
  Where encryption is infeasible, the rule allows compensating controls, but only ones reviewed and approved by the Qualified Individual. Record that approval.
- [ ] Multi-factor authentication for anyone accessing any information system
  The only exception is an equivalent or stronger control the Qualified Individual has approved in writing.
- [ ] How the firm evaluates the security of software and services it did not build
- [ ] Secure disposal within two years of last use, unless the law or a business need requires keeping it
  The rule also requires a periodic review of the retention policy. Your own retention obligations still apply: the two-year rule yields to information "required to be retained by law or regulation".
- [ ] Change management procedures
- [ ] Monitoring and logging of what authorized users do with customer information

TESTING AND MONITORING — §314.4(D)

- [ ] How the key controls are regularly tested or monitored
- [ ] Continuous monitoring, or else annual penetration testing and six-monthly vulnerability assessments
  A firm with information on fewer than 5,000 consumers is exempt from this paragraph, §314.4(d)(2), but not from regular testing or monitoring under (d)(1).
- [ ] The dates and results of the last tests, and what was fixed
- [ ] Extra tests after material changes to the firm's operations or systems
  Where the six-monthly vulnerability assessments apply, the rule also requires one after material changes to operations or business arrangements.

STAFF AND TRAINING — §314.4(E)

- [ ] Security awareness training for all staff, updated for the risks the assessment found
- [ ] Who manages information security, in the firm or at a provider
- [ ] How security staff keep current with threats and countermeasures

- [ ] A signed acknowledgement from each employee and contractor
  Publication 5708 includes one as Attachment D, and suggests renewing it at each annual training.

SERVICE PROVIDERS — §314.4(F)

- [ ] Every service provider with access to customer information, and what each holds
- [ ] How each was selected as capable of maintaining appropriate safeguards
- [ ] The contract terms that require each provider to maintain those safeguards
- [ ] When each provider was last assessed, and the result
  The rule asks for periodic assessment based on the risk each provider presents. A document portal, a tax software vendor and an outsourced IT provider all belong on this list.

INCIDENT RESPONSE AND NOTIFICATION — §314.4(H) AND (J)

- [ ] The written incident response plan, with its goals and internal response process
  Firms holding information on fewer than 5,000 consumers are exempt from the written plan requirement (§314.6). The FTC notification requirement below still applies.
- [ ] Roles, responsibilities and who has authority to decide what
- [ ] Internal and external communications, including who speaks for the firm
- [ ] How weaknesses are fixed, and how incidents are documented and reported
- [ ] Review and revision of the plan after an incident
- [ ] FTC notification within 30 days of discovering an event affecting 500 or more consumers
  Required since May 13, 2024 for unencrypted customer information acquired without authorization, on the FTC's online form.
- [ ] Who else to notify, including your IRS Stakeholder Liaison and state tax agencies
  Publication 4557 asks preparers to report client data theft to their local IRS Stakeholder Liaison, and to the states they file returns in.

REVIEW AND REPORTING — §314.4(G) AND (I)

- [ ] What triggers a revision, such as test results, a new office or a new system
- [ ] Changes made after each risk assessment, and the reason for each
- [ ] The Qualified Individual's written report, at least annually, to the owners or a senior officer
  The report covers the program's status and material matters such as risk decisions, provider arrangements, test results and security events. Firms under the 5,000-consumer threshold are exempt (§314.6).

- [ ] [Firm name]'s record of each review, with the date and the changes made

Supplied as-is, with no guarantee. This template is provided for general information only. It is not legal advice and it is not a substitute for it. Have your own legal adviser review it, and adapt it to your practice and your jurisdiction, before you use it with a client. FirmHello accepts no responsibility or liability for any use made of this document.