Chapter 1: Written Information Security Plans and Protecting Client Data

Note. Corrections were made to this workbook through January of 2024. No subsequent modifications were made. For terms used in this chapter, see the **Acronyms and Abbreviations** section following the index.

For your convenience, in-text website links are also provided as short URLs. Anywhere you see **uofi.tax/xxx**, the link points to the address immediately following in brackets.

About the Author

John W. Richmann, EA, is a Tax Materials Specialist at the University of Illinois Tax School. Prior to joining Tax School in 2021, he owned a tax practice in St. Charles, Illinois, and held positions in private industry and consulting firms. John earned a Masters Degree in Business Administration from the University of Texas and an electrical engineering degree from the Massachusetts Institute of Technology.

Other chapter contributors and reviewers are listed at the front of this book.

INTRODUCTION

The consequences of a client data breach threaten the potential loss of a business, a life's work and calling, and much more. IBM Security estimated that the average total cost of a data breach in 2022 was $4.65 million.[1] This estimate includes notification, responses after the breach occurs, detection and escalation costs including forensic and other investigations, and lost business. The magnitude of these costs is a keen motivator for a tax practice to prepare a written information security plan (WISP).

When it compromises client data, a data breach can fracture client relationships, friendships, and even family relationships. A plan to protect a tax practice's data is, therefore, a plan to protect the network of relationships that constitute the practice.

This chapter focuses on creating a WISP that is useful for managing a tax practice's security. Although the IRS has provided a standard template, the management of each tax practice needs to assess the unique risks it faces. The firm must implement its own WISP to address those risks.

LEGISLATIVE MANDATES

The requirement for tax practitioners to have a WISP originates in the Gramm-Leach-Bliley Act (GLBA). Tax practitioners are considered **financial institutions** under 16 CFR §314.2(h)(2)(viii), which reads,

> *An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 USC 1843(k)(4)(G).*

Therefore, the Federal Trade Commission (FTC) requires all tax preparation services to have a WISP at all times from the inception of their firms to present.[2] The required elements for a WISP are described in 16 CFR §314.4 and are listed in Appendix B at the end of this chapter.

Because this portion of federal regulations brings tax preparation services under FTC control, tax practitioners are subject to the requirements within the GLBA. Following the GLBA's Safeguards Rule,[3] they must implement safeguards protecting their tax clients' **nonpublic** personal information. A small tax practice has the same obligation to plan its data security as a large money center bank. Large firms commonly have established written plans for dealing with different contingencies. Numerous employees typically assemble these documents, with each employee's work reflecting their responsibilities or their respective departments' responsibilities.

In contrast, a single individual likely fills multiple roles in a small tax practice. Aware of this burden on such businesses, the IRS developed a template for a small-scale WISP, contained in IRS Pub. 5708, *Creating a Written Information Security Plan for your Tax & Accounting Practice*. While this WISP template may be insufficient for larger firms having personnel with more distributed responsibilities, it provides small tax practices with a start for complying with the law.

NEW REGULATIONS

In October 2021, the FTC updated the Safeguards Rule after a 2-year process of proposed rulemaking, public commentary, and evaluation by the FTC's five commissioners.[4] The proposed changes stipulated the inclusion of more detailed information in the information security plans, that tax practices encrypt all customer data, and that they implement controls to prevent unauthorized users from accessing customer information.

---

1. *Cost of a Data Breach Report 2022,* p. 5. Aug. 1, 2022. IBM Security®. [www.ibm.com/downloads/cas/3R8N1DZJ] Accessed on Mar. 24, 2023.
2. 16 CFR §§314.3 and 314.5.
3. 16 CFR §314.
4. *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches*. Lincicum, David. Oct. 27, 2021. Federal Trade Commission. [www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data] Accessed on Feb. 15, 2023.

After the GLBA amended requirements, the FTC proposed two additional regulations implementing GLBA amendments that are effective June 9, 2023.[5] These two changes require financial institutions, including tax return preparers, to report to the FTC any data breaches in which the information of at least 1,000 consumers is "reasonably likely" to occur or has occurred. The tax return preparer must report the event to the FTC as soon as possible and no more than **30 days after its discovery.**[6] The preparer report must make the filing on the FTC's website, **www.ftc.gov**, and it must include the following.[7]

- Name and contact information of the reporting financial institution
- Description of the types of information involved in the security event
- Date or date range of the security event, if ascertainable
- General description of the security event

PENALTIES FOR VIOLATING IRC §7216

Unauthorized disclosure of taxpayer information under IRC §7216 carries substantial penalties, including criminal penalties for disclosures by tax return preparers of tax information. Violations of this Code section can trigger penalties of up to **$100,000 plus** prosecution costs. A violation may also result in up to a year of **prison time.** The law attaches severe penalties for the improper disclosure of taxpayer information, providing a solid incentive to protect this information from any threats that could result in its release.

Practitioner Planning Tip

A data breach will be considered a violation of §7216 if a proper WISP was not implemented. It is imperative for even sole practitioners to develop a WISP. Ignoring the requirement to maintain a WISP could be considered willful and reckless, subjecting the practitioner to the fines and penalties mentioned previously.

Note. A proper disclosure includes a formal consent in writing by the party whose data the tax practitioner is disclosing. Although a **§7216 disclosure consent** is normally done with a signature on paper, they may also sign electronically in some circumstances. IRC §7216 stipulates the required language in the consent form and even the minimum size of the type.

5. See 16 CFR §§314.4 and 314.5.

6. 86 Fed. Reg. 70,062 (Dec. 9, 2021).

7. 86 Fed. Reg. 70,062–70,067 (Dec. 9, 2021); *Compliance deadline for certain revised FTC Safeguards Rule provisions extended to June 2023.* Fair, Leslie. Nov. 15, 2022. Federal Trade Commission. [www.ftc.gov/business-guidance/blog/2022/11/compliance-deadline-certain-revised-ftc-safeguards-rule-provisions-extended-june-2023] Accessed on Mar. 21, 2023.

CREATING A WISP[8]

A WISP contains training requirements, evaluations of information systems, how to detect and manage system failures, as well as other items to help protect tax professionals and their clients from their personal information being compromised. The FTC sets and enforces data safeguard regulations for tax practitioners. Tax practitioners who fail to create and enact a WISP may be subjected to an FTC investigation.

A tax practice should adapt its WISP to the company's size, the type of activities in which the company engages, how complex the company is, and the sensitivity of the customer data it maintains. The FTC requires each entity to do the following in its WISP.[9]

- Designate one or more employees to coordinate its information security program
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks
- Design and implement a safeguards program, and regularly monitor and test it
- Select service providers that can maintain appropriate safeguards by ensuring that their contract requires them to maintain safeguards and oversee their handling of customer information
- Evaluate and adjust the program considering relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring

> **Note.** Tax practitioners must acknowledge the requirement for data security plans annually when they renew their practitioner tax identification number (PTIN). The tax practitioner cannot renew their PTIN unless they select the checkbox acknowledging their awareness of the need for a data security plan to provide data and system security protections for all taxpayer information.

The IRS intends the WISP to serve three important functions for tax practices.

1. The WISP is a tool to ensure the security and confidentiality of the personally identifiable information (PII) that a tax firm receives.
2. The WISP helps tax practices protect PII against threats to its integrity.[10] Not only does the FTC require financial institutions, including tax practitioners, to plan for the security of the data clients give them, but they must also ensure that its content is not available to unintended persons. In addition, tax practitioners must ensure that the PII is not corrupted while in the custody of the tax practice.
3. The WISP guides the tax practice in protecting PII from access or use that would create a substantial risk of identity theft or some other use that would harm the person identified in the PII.

---

8. IRS Pub. 5708, *Creating a Written Information Security Plan for your Tax & Accounting Practice*; IRS Pub. 4557, *Safeguarding Taxpayer Data*.
9. IRS Pub. 5708, *Creating a Written Information Security Plan for your Tax & Accounting Practice.*
10. *Gramm-Leach-Bliley Act*, PL 106-102, §501(b).

WISP TEMPLATE[11]

IRS Pub. 5708 lays out the requirements for a WISP, and includes a sample template, as well as samples of important attachments to the plan. A WISP should focus on the following.

- Employee management and training
- Information systems
- Detection and management of system failures

The WISP template recommends that tax practices provide each employee a copy and that after examining the WISP, each employee acknowledge their training and understanding of it in writing. The IRS anticipates that some employees may negligently violate either the letter or the spirit of the plan, suggesting that these steps may provide a mechanism for enforcing accountability. This sign-off process is not a "one-and-done" experience. The IRS anticipates that firms conduct this sign-off process regularly as they review and update their WISP. The IRS suggests that tax practitioners store a copy offsite in a physical location or on the Internet.

The IRS suggests that practitioners distribute documents in PDF or Word format for readability, with no mention of a hand-written WISP.

The template identifies the individuals responsible for data security, the risks the firm faces, and the assets the firm owns. A WISP includes the following seven sections.

1. Define the WISP's objectives, purpose, and scope, collectively constituting a preamble for the document
2. Identify responsible individuals
3. Assess risks
4. Inventory hardware
5. Document safety measures in place
6. Draft an implementation clause
7. Attach any ancillary procedures, including a record retention policy, rules of behavior and conduct safeguarding client PII, and security breach policy

The purpose of the WISP is to accomplish the following goals.

- Protect client data from threats to its security
- Maintain the confidentiality of clients' PII
- Secure the PII from any unauthorized access that results in a substantial risk of identity theft, fraudulent use, or harmful use of this data

> **Caution.** There is obvious judgment involved in discerning substantial risk. However, the level at which the tax practitioner sets the bar here could have legal consequences if a data breach occurs and a federal agency finds the practitioner did not comply with their own standards set forth in the WISP.

11. IRS Pub. 5708, *Creating a Written Information Security Plan for your Tax & Accounting Practice*.

Practitioner Planning Tip

It is probably wise to state in the WISP's preamble that its purpose is to fulfill requirements imposed on the firm by the GLBA. It should also state that it sets a standard for evaluating the effectiveness of measures taken to safeguard data held in the firm's custody.

PERSONALLY IDENTIFIABLE INFORMATION

In the WISP template, the objective section identifies five specific types of data elements that become PII when combined with a taxpayer's first name and last name (or first initial and last name). These data elements are classified as follows.

1. Information that fundamentally identifies an individual who is a U.S. person, including their social security number (SSN), date of birth, and employment data
2. State-issued identification information, including driver's license information or other state-issued IDs
3. Income data, data from tax returns, data from retirement plans, data about assets that the taxpayer owns, and data about investments that a tax client owns
4. Information of **item 3** extended one more level by including the following
    a. Account numbers
    b. Credit and debit card numbers, possibly with security codes
    c. Access codes
    d. Personal identification numbers
    e. Passwords associated with a tax client's financial accounts
5. Taxpayer's contact information, such as a phone number and email address

Practitioner Planning Tip

Practitioners may wish to avoid storing specific credit card and debit card data to limit the potential compromise of client information.

What is Not PII

It is also important to recognize which data is not considered PII. It does not include information from public sources, such as the following.

- Mailing address
- Phone directory listing
- Data available from government records lawfully available to the general public

Example 1. As an enrolled agent, Gregory has operated his tax practice as a sole practitioner for many years. About 10 years ago, he started scanning all records that a client brings so that he could reconstruct how he had prepared a tax return if needed.

Two of Gregory's clients, Herb and Wendy, are a married couple with two children under the age of 17. They own their home and are registered to vote in a state that discloses home ownership and sales prices. Gregory scans the following information.

- Drivers' licenses
- Home and cell phone numbers
- Birth certificates of children
- School and medical records for children, establishing their addresses
- Marriage license
- Forms W-2, *Wage and Tax Statement*
- Forms 1099
- Evidence of contributions to §529 accounts for each child

Their income is considered PII, as this information is not available from publicly available sources. The other information in the documents above is also considered PII, with the likely exception of Herb and Wendy's home address, because this information is available from public sources due to their owning their home and being registered voters.

Access to PII

Access to PII should be restricted to people that require access for their direct responsibilities. Within the tax practice, only individuals with responsibility for a particular client should be able to view that client's data. Outside of the tax practice, clients should be able to view their own data but not that of other clients.

Example 2. Stan owns a tax practice in Illinois. On June 15, one of his employees, Stacey, leaves the firm for a better opportunity. Stan's WISP states that employee access to client PII is to be removed immediately upon leaving employment, but Stan forgets to remove Stacey from the document management system until the time of his normally scheduled monthly review on June 25.

One of Stacey's new clients, Chuck, is divorced and races against his ex-wife Mary (a client of Stan) every year to file first to claim their children. On June 20, Stacey logs on to Stan's tax software (to which she still has access), and checks Mary's e-file status. Stacey notices that Mary's return has not yet been filed, so she quickly claims the dependents on Chuck's return and e-files it.

When Stan subsequently goes to file Mary's return, the IRS rejects it. Stan has to track down why it was rejected and discuss alternatives with Mary.

This situation could possibly have been avoided if Stan had followed his own WISP and immediately terminated Stacey's access to the firm's systems when she quit.

Security Management by Group. Providing each employee in a tax practice with their own security and permissions may seem like a lot of work. Indeed, it is, but that is not the only problem. It is easy to leave a security gap when each employee is treated separately, possibly weakening the entire WISP. Fortunately, most secure software streamlines this process by allowing the creation of security groups that can limit user account permissions to those necessary to perform their jobs, but no more.[12]

The tax practice's data security coordinator (explained in detail later) can place employees with similar needs to access PII in their own security group. In turn, the security permissions are set at the group level, giving all group members the same access privileges to data and the same window during which they can log in to the local network. Even in a small practice, management can anticipate the need for at least three security groups.

- Employees, having limited access to PII based on their client responsibilities
- Management, having unlimited access to PII
- Network administrators, having broad access to the functions of the network, but possibly limited access to PII

Example 3. Use the same facts as in **Example 2,** except that Stan's network administrator sets up the following four security groups on the network.

- Office Administration
- Tax Professional
- Management
- Network Administration

The network administrator provides Stan with two logins, one of which is in the management group, which he uses to review tax returns and financial statements. Because Stan has basic network administration skills, the network administrator also gives him a login to the network administration group, which Stan can use to administer the network on an emergency basis if the network administrator is unavailable. Stan's management login is deliberately not given these capabilities, preventing Stan from inadvertently making changes to the network.

On June 18, Stan notices that Stacey's user ID is still enabled, even though she left the firm several days earlier. Stan removes Stacey from the Tax Professional security group and then disables her user ID after verifying that she did not use her user ID to access the system since leaving the firm.

12. *Recommended Best Practices for Administrators: Identity and Access Management*, p. 8. Feb. 27, 2023. National Security Agency and Cybersecurity & Infrastructure Security Agency. [media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF IDENTITY AND ACCESS MANAGEMENT RECOMMENDED BEST PRACTICES FOR ADMINISTRATORS PP-23-0248_508C.PDF] Accessed on Mar. 24, 2023.

RESPONSIBLE INDIVIDUALS AND SPECIFIC POLICIES

The WISP template identifies two individuals with specific responsibilities, a data security coordinator and a public information officer.

Data Security Coordinator[13]

The data security coordinator is responsible for the overall implementation of the WISP, ranging from daily operating procedures to periodic training, even requiring third-party service providers to adhere to security measures in the WISP. Perhaps most importantly, the data security coordinator identifies where data is stored.

The IRS suggests the following responsibilities for the data security coordinator.

- Implementing the WISP, including daily operational protocols
- Identifying all data repositories that are subject to the WISP protocols, designating them as secured assets, and ensuring access to this data is restricted
- Verifying that every employee has completed recurring information security training
- Monitoring and testing employee compliance with the WISP's policies and procedures
- Evaluating the ability of third-party service providers to comply with appropriate security measures within the WISP
- Reviewing the scope of the security measures in the WISP at least annually or when a significant change in business practices occurs, particularly if the change potentially affects PII integrity
- Conducting an **annual** training session for all owners, managers, and independent contractors, at which all are required to certify their attendance and their familiarity with the requirements for protecting PII

Public Information Officer

The public information officer is responsible for disseminating information about a data breach to a wide range of outside entities, from law enforcement agencies to clients to news media. The public information officer role becomes prominent if the company's data is compromised. This individual is the firm's designated spokesperson in the event of an adverse event that possibly involves a compromise of PII.

The public information officer oversees the following.

- All client communications, whether by phone conversation or by writing
- All communication with law enforcement agencies

> **Caution.** The tax practice owner may want to consult an attorney for guidance regarding communication with law enforcement agencies.

- All releases to news media
- All information released to business associates, nearby businesses, and trade associations

> **Note.** The role of public information officer is not mentioned in the FTC's amended regulations.[14] The notes following the WISP indicate that the IRS expects that the data security coordinator and the public information officer are separate individuals. However, in many small tax practices, this segregation of duties is not feasible.

13. The FTC's regulations refer to the data security coordinator as a "qualified individual." These regulations appear in Appendix B at the end of this chapter.

14. *Standards for Safeguarding Customer Information*. Dec. 9, 2021. Federal Trade Commission. [www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information] Accessed on Feb. 15, 2023.

RISK ASSESSMENT[15]

The WISP template contains two sections on risk mitigation. The first covers **inside-the-firm risks**, such as collecting PII and holding employees accountable for complying with the firm's implementation of the WISP. The WISP also covers **outside-the-firm risks.**

INSIDE-THE-FIRM RISKS

The WISP template addresses policies and procedures a tax firm can implement to reduce risks to PII records being compromised from within the firm.

Record Retention Policy

A **record retention policy** documents a tax practice's policy covering how long the firm should retain client records before destroying them. The longer a tax practice retains PII, the greater the risk of that data being compromised. Documents should be expunged upon reaching the end of their retention period. To expunge paper documents, the firm can either shred them or return them to the taxpayers who provided them. Electronic documents can be "electronically shredded" (a more permanent and secure form of destruction than simple file deletion).

Caution. Document destruction practices have legal consequences that may sometimes require a tax professional to consult with their legal counsel.

Note. Deleting paper documents can be time-consuming. A tax practice's staff can readily delete electronic data, provided operators can see its expiration, or its document management system can delete it automatically.[16] Some document management systems enable operators to set lifetimes for a particular document type.[17]

Example 4. Joseph owns a small tax practice that employs a few seasonal tax preparers and a year-round office manager. He distributes his firm's record retention policy with the annual engagement letter and organizer in early January.

Following the firm's record retention policy, the office manager ensures that the scanned documents in the document management system are labeled with an expiration date seven years after the due date of each year's returns. Consequently, they can delete or destroy information used to prepare 2021 tax returns after April 18, 2029. Their tax practice likely filed these individual returns on or before April 18, 2022.

15. IRS Pub. 5708, *Creating a Written Information Security Plan for your Tax & Accounting Practice*.

16. *How to delete old documents from a site using retention policies.* Zelfond, Gregory. Aug. 25, 2020. Sharepoint Maven. [sharepointmaven.com/how-to-delete-old-documents-from-a-site-using-retention-policies/] Accessed on Feb. 15, 2023.

17. *IBM Content Manager, Version 8.5.0.3*. 2015. IBM Corporation. [www.ibm.com/docs/ko/content-manager/8.5.0?topic=policies-retention-expiration] Accessed on Feb. 15, 2023.

Example 5. Patrick owns a tax practice, employing only Kennedy, a seasonal office manager, during tax season. Kennedy has worked for Patrick for five years, starting when the digital document management system was implemented. The firm has a written policy of retaining documents for five years, and some documents that Kennedy scanned when first working for Patrick have reached expiration. She receives alerts to destroy those documents electronically.

While giving the documents one last review, Kennedy notices that some expired paper documents pertain to pending litigation. Kennedy alerts Patrick to the significance of the expired documents. He contacts the firm's attorney, who instructs Patrick to retain the documents because of the likelihood of a court order pertaining to them.

Caution. Keeping client information longer than required can create a legal problem if a client's information is used to incriminate them. An exception to this point may be a practitioner's permanent files for each client.

PII Disclosure Policy

The **PII disclosure policy** imposes several important restrictions on a tax practice's maintenance of client PII. According to the WISP template, nonemployees may not be present in an office area where client information is physically stored unless an employee accompanies them. As one example, this provision has the practical effect of requiring an employee to be present when the midnight cleaning crew does its work.

Practitioner Planning Tip

To satisfy the requirement that visitors are never unattended, tax practitioners employing an outside cleaning service may consider reviewing the contract with the cleaning service for the hours the service works to ensure that an employee can monitor them.

PII should not be present on an employee's desk when the employee is not working. The WISP template addresses this by stipulating that "employees are trained to keep all paper and electronic records containing PII securely on premises at all times." The tax practitioner preparing the WISP may decide to make this more explicit.

Employees working remotely check out the records containing PII, which may be stored on "solid state drives, and removable or swappable drives, and USB storage media." Only the minimum data necessary for remote work should be removed from the business premises. This is a challenging requirement in the new era of remote work. A tax practitioner often accesses client data through the public Internet, probably through a cloud-based document management application. The PII disclosure policy in the WISP template stipulates that no media, either paper or electronic, should be present in an unattended car, in a home, or in some other location that may not be secure.

Practitioner Planning Tip

Practitioners may consider changing the language from the template to allow an employee who is driving a long distance with client information to stop at a rest area to stretch their legs. Driving a long distance without a break is unreasonable if the reason for denying a break is the presence of PII in the employee's vehicle.

The template provides for sharing information with outside tax authorities and other tax and legal advisors who may assist the tax practice in the normal course of work. It acknowledges that information technology (IT) firms may occasionally see PII while performing their work. It also permits sharing of PII with the following outside entities who encounter PII in the normal course of business.

- IT support firms
- Tax software vendors
- Bookkeeping services
- Payroll services
- CPA/EA firms
- Legal counsel
- Business advisors
- Law enforcement agencies
- Other governmental agencies

The WISP limits the permitted disclosure of information to the minimum necessary to meet the business need. These individuals must comply with the standards of the WISP, at the very least. Although the WISP template provides exclusions from this requirement for tax software vendors and governmental agencies, it does so with the expectation that they comply with even stricter regulations.

The PII disclosure policy includes document safety measures that seek to secure PII pertaining to the tax practice's clients, employees, and contractors. The policy describes principles for data collection and retention, such as the following.

- Making sure that the person to whom PII is being disclosed is really the person intended by the client
- Restricting access to places where PII is stored
- Reviewing the security measures contained in the WISP

The policy also requires the tax practice's managers to define the minimum amount of PII it requires and identify who in the practice should have access to it. Thus, a tension exists between minimizing data collection to minimize data risks, even while the IRS periodically enlarges due diligence requirements, which necessarily increases the volume of data required.

The first item of business for a tax practitioner whose client has asked them to disclose their PII to a third party is to verify the third party's identity.

Example 6. While refinancing his principal residence, Mark asks his tax practitioner, George, to send Mark's mortgage broker a copy of his last two tax returns. George sends Mark a §7216 disclosure consent, which Mark promptly signs and returns. George also asks Mark to verify that he is providing the information to the correct party.

Mark provides George with the broker's work phone number and email address. Soon George's receptionist receives a phone call from an individual claiming to be a mortgage broker working with Mark. George does not accept the call. Instead, George calls the number Mark provided to ensure that he speaks with the correct person. Before calling, George performs an Internet search to verify the phone number Mark provided is associated with the broker. George then calls the mortgage broker, speaks directly with the individual whose name Mark provided, and sets up a means to securely provide the tax returns.

Personnel Accountability Policy

Without compelling the activities of individuals, a WISP would be without consequences and, therefore, without effect. The **personnel accountability policy** requires individual employees and contractors to acknowledge receipt of the WISP and their ongoing compliance with it. Not only are all employees required to be trained on the WISP, but they are also subject to periodic reviews by the data security coordinator to verify their compliance. The WISP template encourages employees to report security risks:

- To the data security coordinator, or
- To the firm's principals or owners if the data security coordinator is the source of the security risk.

The tax practice is responsible for the following.

- Creating general rules of behavior and conduct regarding the security of PII
- Screening of procedures before granting existing employees access to PII
- Conducting background checks on new employees

Additionally, the firm should consider requiring employees who have PII access to execute nondisclosure agreements. This policy ensures employees know their responsibilities to secure PII by applying the following.

- Removing files containing PII from their desks when they are not present at the desk and requiring the electronic storage of PII to be either secured by password or encryption, if not both ("clear desk policy")
- Locking computers when employees are not present at their desks ("clear screen policy")
- Removing paper files and other PII sources to locked storage, either in a file cabinet or their locked desks

As noted previously, tax practitioners must encrypt all customer data per the Safeguards Rule. The requirement to encrypt data can be waived if a qualified individual, presumably the tax practice's data security coordinator, permits an "alternative means to protect customer information."[18] With a notice dated November 15, 2022, the FTC announced the delayed effectiveness of this rule until June 9, 2023.[19] This notice cited a "reported shortage of qualified personnel" capable of implementing the security upgrades required by the new rule. FTC Commissioner Wilson stated her agreement with the delay. Still, her opinion is that the requirements impose "new onerous, misguided, and complex obligations" with neither a significant reduction in data security risks nor consumer benefits.[20]

---

18. 86 Fed. Reg. 70,286.

19. *Compliance deadline for certain revised FTC Safeguards Rule provisions extended to June 2023*. Fair, Lesley. Nov. 15, 2022. Federal Trade Commission. [www.ftc.gov/business-guidance/blog/2022/11/compliance-deadline-certain-revised-ftc-safeguards-rule-provisions-extended-june-2023] Accessed on Nov. 17, 2022; *Standards for Safeguarding Customer Information*. Nov. 18, 2022. Federal Trade Commission. [www.ftc.gov/system/files/ftc_gov/pdf/Final-Effective-Date-Notice.pdf] Accessed on Nov. 18, 2022.

20. *Concurring Statement of Commissioner Christine S. Wilson*. Wilson, Christine S. Nov. 14, 2022. Federal Trade Commission. [www.ftc.gov/system/files/ftc_gov/pdf/Concurring Statement of Commissioner Wilson SG Rule.pdf] Accessed on Nov. 18, 2022.

The personnel accountability policy provides for discipline or termination of employees who deliberately disclose PII to unauthorized parties. It also requires the revocation of computer system access when employees terminate, either willfully or otherwise. This requirement includes the termination of externally hosted computer systems in the cloud and voicemail, which may require significant time if there are many disconnected systems. They must also surrender their keys, badges, and other means of physical access to the tax practice's office.

Security. The data security coordinator must maintain lists of all lock combinations, passwords, and keys. The WISP may restrict the data security coordinator to only having custody of passwords required to manage the network. The data security coordinator should not possess passwords that individual employees use, which would be a security breach because employees should not share their passwords with anyone.

A WISP should specify that file cabinets be locked when not actively used. This protects against any unplanned visits from persons not on tax practice staff.

> **Note.** This policy may lead to an office **closing procedure** to ensure that PII is secure and the office itself is physically secure each time tax practice personnel vacate it. A closing procedure is a systematic means of ensuring that file cabinets and computers are locked, as well as the office's external doors. This procedure could take the form of a daily checklist.

> **Note.** The password requirement effectively mandates that the data security coordinator use a password manager. An analysis and comparison of various password managers is beyond the scope of this chapter. More information about password managers, including reviews of features, is available on various tech websites.

Example 7. Thad owns a tax practice and rents an office on the second floor of an office building. Thad's office has several file cabinets containing clients' PII, and the office closing procedure includes verification that all file cabinets are locked.

Thad is at home on a hot Sunday afternoon in July, enjoying a televised baseball game. He is interrupted by a message from his office landlord, who occupies a first-floor office in the same building. Already an hour old, the message informs Thad that water is leaking into the landlord's office from Thad's office above it. Because structural damage to the building is a possible result, the message states that the landlord must immediately enter Thad's office to determine the source of the leak.

As Thad listens to the message, he receives a phone call from the landlord, who wants to discuss condensation from the air conditioning that cannot drain. The condensation has formed a pool of water in Thad's office. Because the last person to leave Thad's office locked the file cabinets as they left, Thad did not have to disclose the breach to clients or to regulatory authorities.

Reportable Event Policy

The purpose of the **reportable event policy** is to establish a communication plan for the tax practice's response to adverse data security events. Before any event happens, this policy recommends the data security coordinator maintains all prudent and necessary insurance and legal counsel on retainer for the firm, including the following.

- Data theft insurance
- Cyber theft insurance riders
- Retention of legal counsel

The reportable event policy requires the data security coordinator to review any security incident and analyze the nature of the event and the firm's response to it. As a result of the review, the firm must record any changes to its WISP.

IRS protocols require the tax practice to notify the following agencies following a data breach.

- IRS stakeholder liaison
- State law enforcement authorities
- Local law enforcement authorities

Although the WISP template explicitly charges the data security coordinator with this responsibility in the reportable event policy, this activity aligns with the responsibilities delegated to the firm's public information officer.

The notes following the WISP template state the need for the tax practice to construct an inventory of all data containing PII. This inventory might include the following devices.

- Computers
- Servers
- Network devices
- Cell phones
- Printers, scanners, and copy machines
- Modems
- Routers

As shown in Appendix A at the end of this chapter, Attachment E to the WISP template provides a 5-column spreadsheet for a tax practitioner to maintain inventory information, including hardware item, location, principal user, in-service date, and when last inventoried.

Cyber Insurance.[21] The FTC recommends cyber insurance coverage that protects against the following threats.

- Data breaches (e.g., incidents involving theft of personal information)
- Cyberattacks on tax practice data held by third parties, including vendors
- Cyberattacks on the tax practice's network
- Cyberattacks occurring anywhere in the world, not just in the United States
- Terrorist acts

Additionally, tax practitioners should consider the following policy endorsements or features.

- Defending the tax practice in a lawsuit or regulatory investigation
- Umbrella coverage
- Provision of a 24/7 breach hotline

21. *Cybersecurity for Small Business*. Federal Trade Commission. [www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf] Accessed on Nov. 10, 2022.

First-party coverage should provide the following.

- Legal counsel to determine tax practice notification and regulatory obligations
- Customer notification and call center services
- Crisis management and public relations
- Forensic investigation services
- Recovery and replacement of lost or stolen data
- Business interruption coverage
- Cyber extortion and fraud coverage
- Coverage for fees, fines, and penalties related to the security breach

Third-party coverage protects a tax practitioner against claims by a third party following a data breach. The coverage typically protects against the following.

- Payments to customers suffering loss
- Claims and settlement expenses relating to disputes
- Losses related to defamation and intellectual property infringement
- Litigation costs
- Costs for responding to regulatory inquiries
- Accounting costs
- Other settlements, damages, and judgments

OUTSIDE-THE-FIRM RISKS

The IRS addresses risks from external sources to PII by recommending a variety of policies and procedures.

Network Protection Policy

A network protection policy incorporates six levels of security that collectively protect the tax practice's network from external threats.

1. Firewall protection, operating system security patches, and all software products should be patched and up to date on any computer accessing the firm's network.
2. System security software, such as antivirus and Internet security software, should be patched with up-to-date modifications and installed on any computer accessing the firm's network.
3. User authentication protocols should require two-factor authentication (2FA), and strong, complex passwords that are changed at least every 90 days. Tax-practice passwords should not be the same as personal passwords.
4. The WISP template requires continuous monitoring of computer systems, enabling prompt detection of unauthorized access to PII data. This activity requires **event logging** on all computers attached to the network. Event logging is a method that computer operating systems use to record everything that takes place on a computer. This record enables system administrators to track events that may have led to a security breach or a system failure.[22]

[22] See *Spotting the Adversary with Windows Event Log Monitoring*. Feb. 28, 2013. National Security Agency/Central Security Service. [cryptome.org/2014/01/nsa-windows-event.pdf] Accessed on Mar. 23, 2023; See also *Event Log*. Rouse, Margaret. May 11, 2015. Techopedia Inc. [www.techopedia.com/definition/25410/event-log-networking] Accessed on Mar. 22, 2023.

5. A tax practice's firewall should "be secured and maintained by the practice's IT services provider" and updated as the vendor indicates. As a practical matter, this rules out consumer router/firewall products commonly available at retail stores. This element mandates the implementation of a firewall on each computer, typically a software-based one.

6. The WISP template requires continuous review and installation of operating system patches. Additionally, the data security coordinator should "conduct a top-down security review at least every 30 days."

Note. In terms of employee time, conducting a complete security review every 30 days is a costly requirement for a small tax practice to implement, especially during tax season.

Practitioner Planning Tip

A tax practice should consider adding to its network protection policy a requirement that all removable storage devices, such as USB drives, be tested for viruses or malware on a computer that is **not** connected to the tax practice's network and has updated antivirus software.

User Access Control Policy

This policy requires user passwords to be changed no less frequently than every 90 days. Additionally, users must have unique passwords and not share passwords or accounts on any computer system, Internet access, or product downloads.

Electronic Exchange of PII Policy

The policy for exchanging PII with outside parties requires that a tax practice not send data by an unsecured medium, such as an unencrypted text message. Some email systems can safely send PII because they use **symmetric encryption.** This method requires the sender and receiver to exchange a password, which they must share through a different medium, such as a phone call or a text message. Banks often use an asymmetric encryption method to send PII through email. **Asymmetric encryption** does not require the parties to exchange a password. Instead, they exchange information using pairs of related digital keys.[23]

While email has greatly facilitated convenient communication between businesses and their customers, it has not been great at facilitating **secure** communication. Secure communication generally requires the exchange of certificates or digital IDs between parties without the use of email. A **digital certificate** authenticates the sender of a message and can be used to encrypt communication between the two parties.[24]

Note. Tax practices may wish to perform a web search for "secure email services" to find services that facilitate the exchange of certificates in providing secure email communication. These services are likely to still require the use of a password known to both parties. Because some of these services are located in other countries, tax practitioners should understand the issues arising from storing data in a country other than the United States, as well as the privacy laws in that country.

---

23. *Public-key cryptography*. Feb. 25, 2023. Wikipedia. [en.wikipedia.org/wiki/Public-key_cryptography] Accessed on Feb. 27, 2023.

24. *Digital Certificate.* Shacklett, Mary and Loshin, Peter. Sep. 2021. TechTarget.com. [www.techtarget.com/searchsecurity/definition/digital-certificate] Accessed on Apr. 12, 2023.

Practitioner Planning Tip

A firm's WISP should grant the tax practice permission to share PII with external firms when necessary to complete tax returns. The disclosures must be done in compliance with Circular 230 and other laws and regulations. This includes court-ordered demands to disclose information.[25]

Secure Portals.[26] A tax practice should communicate a preference for exchanging PII through a secure portal with clients. With a portal, electronic documents are uploaded to a secure storage facility online rather than sent directly through email. Because portals can readily have hefty security, often with 2FA, tax practices can have increased confidence that PII exchanged through this mechanism is secure. Tax practice management should consider a secure portal as a trusted network and protect it with its firewall.

Practitioner Planning Tip

Tax practitioners should consider selecting a portal that integrates with the firm's phones, emails, website, etc.[27] This makes it easier for clients to upload a variety of documents to the secure portal. Additionally, the portal should be integrated with the firm's document management system.

Additional features to consider are cloud-based portals, mobile applications, ability to pay invoices through the portal, custom website address to conform to the firm's brand, and support for multiple and/or large files. Most importantly, the portal should have robust security and encryption.

USB Drives.[28] Although less common than a few years ago, taxpayers may provide data to their tax practitioners on USB drives. While this is a convenient way of exchanging information at an in-person meeting, it is not necessarily secure.

There is a risk of infecting the tax practice's network system, but another risk is present with this exchange of information. A USB drive can hold a large amount of PII. For example, an employee of the tax practice may take home the USB drive to work on a tax return but stops at the grocery store where they lose the USB drive. In this unfortunate circumstance, the tax practice should assume it has disclosed all unencrypted PII on the USB drive. The WISP template requires all USB drives containing PII to have some form of encryption.

---

25. IRC §6103(i).

26. *Protecting Federal Tax Information (FTI) in Web Portals.* Apr. 5, 2023. IRS. [www.irs.gov/privacy-disclosure/protecting-federal-tax-information-fti-in-web-portals] Accessed on Apr. 6, 2023; *Client Portals: A Secure Alternative to E-Mail*. Defelice, Alexandra. Feb. 2020. Journal of Accountancy. [www.journalofaccountancy.com/issues/2010/feb/20092359.html] Accessed on Mar. 22, 2023.

27. *2021 Reviews of Client Portals for Accounting Firms.* Wagner, Garrett, CPA. Feb. 22, 2021. CPA PracticeAdvisor. [www.cpapracticeadvisor.com/2021/02/22/2021-reviews-of-client-portals-for-accounting-firms/40620/] Accessed on Mar. 10, 2023.

28. *Using Caution with USB Drives.* Feb. 1, 2021. Cybersecurity & Infrastructure Security Agency. [www.cisa.gov/news-events/news/using-caution-usb-drives] Accessed on Mar. 22, 2023; *The Risks of Using Portable Devices*, p. 1. Walters, Pennie. 2012. Cybersecurity & Infrastructure Security Agency. [www.cisa.gov/sites/default/files/publications/RisksOfPortableDevices.pdf] Accessed on Mar. 22, 2023.

Wi-Fi Access Policy

The WISP template requires strong encryption on the firm's internal Wi-Fi network. If the firm provides Wi-Fi to guests, they must connect to an entirely separate network. This separation prevents guests from intercepting information on a firm's internal work network.

The policy acknowledges that the tax practice may have devices with wireless network interfaces. These networks commonly connect printers but might also include refrigerators or fax machines. The policy asserts the responsibility of the tax practice to change factory passwords to passwords that the firm assigns.

> **Note.** While changing the factory password may be good practice for protecting the appliance, it does not necessarily protect the tax practice. Tax practices may decide that connecting specific devices is not worth the security risk they present.

Remote Access Policy

The WISP template requires remote access software to encrypt Internet traffic between the remote user and the office and provide 2FA. The WISP template cautions that, "Remote access is dangerous if not configured correctly and is the preferred tool of many hackers."

Despite remote access becoming an industry standard, this is a reasonable warning for even small tax practices to heed. If they do not carefully implement remote access policies, they make their own and their clients' data vulnerable to hostile actors.

> *Organizations should carefully consider the balance between the benefits of providing remote access to additional resources and the potential impact of a compromise of those resources. Organizations should ensure that any internal resources they choose to make available through remote access are hardened appropriately against external threats and that access to resources is limited to the minimum necessary through firewalling and other access control mechanisms.*[29]

Additionally, the remote access policy should include a "no after-business-hours remote access policy." Hackers often capitalize on the network not being monitored by employees during the off-hours to hack the local network.

> **Example 8.** Based on input from his cyber insurance provider, Frank restricts the hours that all staff other than he can log into the firm's computer network. The administrator sets up a schedule that allows all employees to log in to the network between 7:30 AM and 7:00 PM from January 15 until April 1 and from 7:30 AM until 10:00 PM from April 2 until April 18. Frank is permitted to log in at all hours throughout the year.

> **Note.** If a tax practice permits remote work, it may consider providing employees with company-owned computers to ensure they have appropriate security software.[30] These devices should have a secure virtual private network (VPN), antivirus, and other security software installed to protect the computers and the practice's network. Because employees may use mobile devices in less-controlled environments, the practice may consider a special agreement for employees to whom mobile equipment is assigned. These agreements could include the following employee requirements to prevent data theft.
>
> - Prevent use by nonemployees
> - Lock the device when not using it
> - Report loss immediately if the device is misplaced or stolen

---

29. *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, p. 4. Souppaya, Murugiah and Scarfone, Karen. Jul. 2016. National Institute of Standards and Technology. [nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-46r2.pdf] Accessed on Mar. 23, 2023.

30. IRS Pub. 4557, *Safeguarding Taxpayer Data,* p. 7 (2021).

Remote Access Options.[31] Tax practice owners and managers can choose from multiple remote access options. **Remote desktop protocol** (RDP) allows a remote user to take over a physical computer in the office of the tax practice.

Because RDP effectively takes over one of the computers on the network, employees in the office can generally observe actions that the remote user is taking. It permits remote employee access to applications that may only be authorized to run on the computer which they have set up for remote access. This access also makes the WISP requirement to restrict remote login hours more reasonable. RDP services generally encrypt traffic, but a tax practice should vary the existence and strength of any encryption used. However, there is a risk with RDP that the wrong employees observe the legitimate actions of an authorized remote user.

An alternative to RDP is to set up **VPN access** to the tax practice's network. This allows the remote computer to function as a computer on the local network, although it may be thousands of miles away. Persons working in the office may not be able to directly monitor remote activity by looking at a computer on a desk. The VPN encryption allows the remote user to access the tax practice's private network through the public Internet. Once connected, it accesses the tax practice's network through a VPN server, which is a gate to restrict traffic and only allows permitted users access to the network. Organizations implementing a VPN have additional factors to consider, such as the following.[32]

- Employees working remotely may receive a greater number of phishing emails.
- If the tax practice does not use 2FA, it is more vulnerable to phishing attacks.
- VPNs are more likely to be used around the clock, making it more difficult to apply security updates, perhaps increasing the likelihood they will not be installed.

A VPN can protect remote computers, even though it adds a level of complexity to the management of the computer. A VPN protects remote computers by encrypting information the user transmits over the Internet and also by disguising the user's location.[33] Thus, if employees use their company computer outside the office but do not need to access the employer's network, they may still wish to use a VPN connection to access the Internet to protect themselves from hostile parties.

Note. This discussion only introduces the importance of including remote access policies in a WISP, not to advise the implementation of a specific remote access mechanism. The leadership of a tax practice should consult a knowledgeable IT services firm with demonstrable experience implementing remote access for advice specific to their requirements. They may wish to review Internet articles from both remote desktop protocol providers and VPN providers, as well as other alternatives for securing remote network access.

Example 9. Cindy is a CPA who often works remotely from her home for a small tax practice. On March 25, she goes to a local coffee house to meet a friend but arrives an hour early to finish some work. After accessing the coffeehouse's network, she immediately connects to her employer's VPN to encrypt all traffic. This precaution complies with the company's remote access policy, which requires using a secure VPN while working remotely, either from home or on a public network. By using the company-supplied VPN, Cindy complies with the requirement in the WISP template to use remote access only with encryption.

Caution. Coffee shops often have unsecured public Wi-Fi networks, but they are also present in airports, hotels, restaurants, and many other public accommodations.

---

31. VPN *vs. RDP: what's the difference?* Markuson, Daniel. Jun. 11, 2022. Nord VPN. [nordvpn.com/blog/vpn-vs-rdp/] Accessed on Nov. 14, 2022.

32. *Enterprise VPN Security*. Apr. 15, 2020. Cybersecurity & Infrastructure Security Agency. [www.cisa.gov/news-events/cybersecurity-advisories/aa20-073a] Accessed on Mar. 23, 2023.

33. *A VPN can protect your online privacy. But there's a catch.* Hautala, Laura. Mar. 29, 2019. CNET. [www.cnet.com/tech/services-and-software/vpn-protect-online-privacy-its-complicated] Accessed on Apr. 6, 2023.

Even mobile device charging stations can be insecure if a user connects their equipment in a manner that allows data connectivity in addition to power charging. Hostile actors may place charging stations in airports that permit them to grab data from connected phones. This practice is sometimes known as "juice-jacking."[34] While traveling, it is recommended to use "power-only USB cables" that do not transfer data, or plug the phone's charger into a dedicated AC power outlet (if available) rather than a charging station. There are also USB data blockers that prevent the exchange of data.[35]

Example 10. Lucy, CPA, takes a vacation on April 20, closing out a tumultuous tax season. Without charging her phone, Lucy leaves for the airport, confident she can find a public charger. She plugs her phone into a public charging station in the airport terminal. The plane bound for Florida arrives late, allowing the phone to charge for two hours.

Unknown to Lucy, the plug not only fills her phone's battery but also installs malware, compromising client information that she had not removed following tax season. Lucy must file a claim with her insurance company on a $300,000 cybersecurity loss.

Example 11. A large national pipeline company, Colonial Pipeline, implemented a VPN after already establishing a complex password policy.[36] However, a group of cybercriminals found an employee's unencrypted password on the server, giving them access to the network through a VPN connection. The company had not implemented 2FA on the specific application. Before 5:55 AM one morning, an employee found a $5 million ransom note. By 6:10 that morning, the company had shut down its entire pipeline system, stretching 5,500 miles, thereby threatening fuel to millions of Americans.

Note. These examples make it clear that a WISP should include provisions for protecting data with a 2FA, a VPN or remote data connection, and even an inexpensive data blocker. Although implementing these tools requires some preparation and expense, they are essential in protecting a company's data. In adopting the WISP template to their practices, the tax practice may wish to consider the costs and benefits of protecting their company's systems.

Caution. Although using a VPN in the United States is legal, some countries, such as the People's Republic of China, prohibit their use.[37] For this reason, a tax practitioner traveling in China, even for vacation, may wish to leave at home all electronic equipment that could be used to connect to any network.[38]

Connected Devices Policy

The WISP template requires all new devices to undergo a thorough security review before connecting to the tax practice's network. This thorough review should check for security patches and password protocols.

---

34. *Do you need a USB data blocker? You do if you use public USB charging stations.* Betts, Anne. Dec. 6, 2021. Packing Light Travel. [packinglighttravel.com/travel-tech/do-you-need-a-usb-data-blocker/] Accessed on Nov. 14, 2022.

35. *How to Safely Use Airport Charging Stations*. Wilton, Thomas James. Oct. 27, 2022. Lifewire: Tech for Humans. [www.lifewire.com/safely-use-airport-charging-stations-4690583] Accessed on Nov. 3, 2022.

36. *Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate*. Wilkie, Christina. Jun. 9, 2021. CNBC. [www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html] Accessed on Nov. 14, 2022; *One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators*. Kelly, Stephanie and Resnick, Jessica. Jun. 8, 2021. Reuters. [www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/] Accessed on Nov. 14, 2022.

37. *Is Using a VPN Legal?* Vigderman, Aliza and Turner, Gabe. Nov. 14, 2022. Security.org. [www.security.org/vpn/legality/] Accessed on Dec. 6, 2022.

38. *Bring a burner to the Olympics, and other mobile device travel safety tips*. Vigliarolo, Brandon. Feb. 3, 2022. Tech Republic. [www.techrepublic.com/article/bring-a-burner-to-the-olympics-and-other-mobile-device-travel-safety-tips/] Accessed on May 25, 2023.

Many AutoRun or AutoPlay features facilitate software installation from a CD-ROM or USB device or to play music from a CD.[39] Unfortunately, this also makes it easy for malware to install itself on a computer. The WISP template attempts to minimize this possibility by requiring AutoRun or AutoPlay to be disabled. Tax practitioners must still check any USB device a client brings for malware.

Example 12. Every year Nancy, the partnership representative of CSQ Partnership, provides Carla, EA with a USB drive containing all records necessary to prepare Form 1065, *U.S. Return of Partnership Income,* and the associated state tax returns. In 2022, Carla implemented a WISP that prohibits USB drives from being connected to its internal network.

When Carla sends out her organizer at the beginning of 2023, she includes a note about her new policy of not allowing USB drives. She provides information on how to set up an account on her secure portal. Before their February meeting, Nancy successfully sets up CSQ's account and uploads all the relevant documents. Nancy and Carla feel secure knowing the information is encrypted and protected on the portal.

Old storage devices, such as disk drives, present a problem when they become obsolete. The WISP template mandates erasure of these devices where possible, or otherwise prevent their ability to connect to other devices.

The WISP template mentions the need for **antivirus software** to be running and licensed. The tax practice's computers must update the virus signatures regularly, and the network must be "tested weekly to ensure the protection is current and up to date" to prevent connected devices from introducing viruses or malware.

Caution. Tax practitioners may also wish to consider how devices themselves may collect data. Because portable devices are so powerful, their owners may unwittingly release information to firms that should not have this data in their possession. This capability also makes the tax practices' policies concerning cell phones and tablet computers particularly important because these devices are likely to have speech recognition software (e.g., Apple's Siri or Google Assistant). The broad availability of artificial intelligence magnifies the risk of data compromise.

Information Security Training Policy

Training personnel is arguably the most important portion of a WISP. If a tax practice's employees do not understand the WISP, they cannot fulfill their responsibilities, making it hard to hold them accountable for appropriately controlling access to data. When a tax practice's management makes regular data security training available, it emphasizes the value it places on the security of customer PII.

Annual training sessions have been the standard for training tax practice employees. Tax professionals may consider holding sessions more frequently.

Credit Card Processing Policy

Although not part of the WISP template, a tax practice should consider how it complies with credit card laws and regulations. The payment card industry (PCI) maintains standards covering the security of credit card information.[40] Some rules restrict credit card processing to a single computer within the firm and prohibit the storage of credit card information. In 2021, the IRS recommended using Transport Layer Security Level 1.3 as a faster and more secure alternative to secure sockets layer (SSL) transmission of any credit card information.[41] Principals of tax practices may wish to review these rules to ensure that their firms are compliant and can access credit card processing networks.

---

39. *AutoRun*. Oct. 13, 2020. Wikipedia. [en.wikipedia.org/wiki/AutoRun] Accessed on Nov. 14, 2022; *The Risks of Using Portable Devices*, p. 3. Walters, Pennie. 2012. Cybersecurity & Infrastructure Security Agency. [www.cisa.gov/sites/default/files/publications/RisksOfPortableDevices.pdf] Accessed on Mar. 22, 2023.

40. *The Prioritized Approach to Pursue PCI DSS Compliance*. Aug. 2022. PCI Security Standards Council. [docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/Prioritized-Approach-For-PCI-DSS-v4-0.pdf] Accessed on Nov. 15, 2022.

41. IRS Pub. 4557, *Safeguarding Taxpayer Data,* p. 16 (2021); *An Overview of TLS 1.3 — Faster and More Secure*. 2023. Kinsta, Inc. [kinsta.com/blog/tls-1-3/] Accessed on Feb. 21, 2023.

ANNUAL CHECKLIST[42]

Each year, a tax practice should review its WISP template, making changes as needed to reflect changes in regulations and in the practice itself. IRS Pub. 4557, *Safeguarding Taxpayer Data,* contains the following checklist that practitioners can use to evaluate and monitor the WISP for their tax practices.

ONGOING	DONE	N/A	Employee Management and Training
☐	☐	☐	The success of your information security plan depends largely on the employees who implement it. Consider these steps:
☐	☐	☐	The success of your information security plan depends largely on the employees who implement it. Consider these steps:
☐	☐	☐	Check references or doing background checks before hiring employees who will have access to customer information.
☐	☐	☐	Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.
☐	☐	☐	Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
☐	☐	☐	Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.) (**IRS suggestion**: passwords should be a minimum of eight characters, the NIST standard. Prevent password sharing; ensure each employee with access to taxpayer accounts uses a unique password.)
☐	☐	☐	Use password-activated screen savers to lock employee computers after a period of inactivity.
☐	☐	☐	Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.

42. IRS Pub. 4557, *Safeguarding Taxpayer Data.*

ONGOING	DONE	N/A	
☐	☐	☐	Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
☐	☐	☐	• Locking rooms and file cabinets where records are kept;
☐	☐	☐	• Not sharing or openly posting employee passwords in work areas;
☐	☐	☐	• Encrypting sensitive customer information when it is transmitted electronically via public networks;
☐	☐	☐	• Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and
☐	☐	☐	• Reporting suspicious attempts to obtain customer information to designated personnel.
☐	☐	☐	Regularly remind all employees of your company's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.
☐	☐	☐	Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
☐	☐	☐	Impose disciplinary measures for security policy violations.
☐	☐	☐	Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures. (**IRS Suggestion**: Deactivate access prior to termination.)
☐	☐	☐	(**IRS Suggestion:** Add labels to documents to signify importance, such as "Sensitive" or "For Official Business" to further secure paper documents.)
			## Information Systems
			Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some FTC suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal:
☐	☐	☐	Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:
☐	☐	☐	• Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.

ONGOING	DONE	N/A	
☐	☐	☐	• Store records in a room or cabinet that is locked when unattended.
☐	☐	☐	• When customer information is stored on a server or other computer, ensure that the computer is accessible only with a "strong" password and is kept in a physically secure area. (**IRS Suggestion:** If using a cloud storage service, use a strong password, multi-factor authentication options and beware of thieves posing as providers.)
☐	☐	☐	• Where possible, avoid storing sensitive customer data on a computer with an Internet connection.
☐	☐	☐	• Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area.
☐	☐	☐	• Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.
☐	☐	☐	Take steps to ensure the secure transmission of customer information. For example:
☐	☐	☐	• When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit. (**IRS Suggestion:** Transport Layer Security 1.3 is newer and more secure.)
☐	☐	☐	• If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.
☐	☐	☐	• If you must transmit sensitive data by email over the Internet, be sure to encrypt the data. (**IRS Suggestion:** Rather than using email, transmit files via Secure File Transfer Protocol (SFTP), successor to File Transfer Protocol (FTP)).
☐	☐	☐	Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule. For example:
☐	☐	☐	• Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
☐	☐	☐	• Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.
☐	☐	☐	• Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.

ONGOING	DONE	N/A	Detecting and Managing System Failures
			Effective security management requires your company to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:
☐	☐	☐	Monitor the websites of your software vendors and read relevant industry publications for news about emerging threats and available defenses.
☐	☐	☐	Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:
☐	☐	☐	• check with software vendors regularly to get and install patches that resolve software vulnerabilities;
☐	☐	☐	• use anti-virus and anti-spyware software that updates automatically;
☐	☐	☐	• maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations;
☐	☐	☐	• regularly ensure that ports not used for your business are closed; and
☐	☐	☐	• promptly pass along information and instructions to employees regarding any new security risks or possible breaches.
			Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to:
☐	☐	☐	• keep logs of activity on your network and monitor them for signs of unauthorized access to customer information;
☐	☐	☐	• use an up-to-date intrusion detection system to alert you of attacks;
☐	☐	☐	• monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and
☐	☐	☐	• insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.
			Take steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs:
☐	☐	☐	• take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet;
☐	☐	☐	• preserve and review files or programs that may reveal how the breach occurred; and

ONGOING	DONE	N/A	
☐	☐	☐	• if feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.
			Consider notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example:
☐	☐	☐	• notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm;
☐	☐	☐	• notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;
☐	☐	☐	• notify the credit bureaus and other businesses that may be affected by the breach. See Information Compromise and the Risk of Identity Theft: Guidance for Your Business; and
☐	☐	☐	• check to see if breach notification is required under applicable state law.
☐	☐	☐	• (**IRS suggestions:** Practitioners who experience a data loss should contact the IRS and the states. Also, consider having a technical support contract in place, so that hardware events can be fixed within a reasonable time and with minimal disruption to business availability.)

EMPLOYEE CODE OF CONDUCT

The WISP template includes a sample written employee code of conduct that provides specific guidelines for protecting clients' PII. The Rules of Behavior and Conduct Safeguarding Client PII as provided by the IRS is included as Attachment B in Appendix A at the end of this chapter.

Email Usage

Employees cannot depend on poor grammar to detect phishing attempts. Instead, employees should call the sender to verify the legitimacy of any links in messages purporting to come from them. Employees can also inspect the web address of the destination link by hovering the computer cursor over a hyperlink in an email. The employee should consider destroying the message if the destination link does not contain a domain related to a trusted source.

Example 13. Cameron expects blank Forms 1099-NEC, *Nonemployee Compensation*, to arrive any day, and he knows the vendor uses WPS to ship them by next-day services. He receives an email from WPS containing the WPS logos and other graphical elements that strongly resemble other emails from the shipper. Because he is anxious to receive the package, he clicks on the link without checking the embedded destination web address. As the link is opening, he notices that the browser window points to the tinyurl.com domain.

Cameron immediately shuts down the browser and informs his firm's data security coordinator of the possible threat per the employee code of conduct in place. Cameron is known to be vigilant regarding email and phishing attempts and is current with the firm's security training. Cameron's managers thank him for reporting the incident and proactively shutting down his computer. They note that his alertness prevented what could have been a virus infection of his computer and potentially the entire company's network.

Note. A tax practice's principals may consider stating in their WISP that an employee reporting a security breach will not be disciplined if the breach is reported promptly. Fear of retribution because an employee mistakenly clicked on a link in an email may result in the employee not reporting security events and, therefore, the threat is not neutralized before it can cause harm.

Internet Usage

The code of employee conduct mandates the segregation of devices for business and personal use. Hence, it would require employees to use personal devices during lunch to check personal email or social media accounts.

Note. If a tax practice maintains a separate network for clients and vendors, it should decide whether it wants employees' personal devices to use it for Internet connections. If a firm's principals decide to permit this, the WISP should provide rules governing the content accessed through its Internet connection.

Personal or Untrusted Storage Devices

Employees should not comingle external storage devices between personal and business devices to avoid introducing malware. As discussed previously, employees should disable any AutoRun or AutoPlay features as well.

Software Copyright and Licensing Integrity

The employee code of conduct instructs employees to avoid downloading software from websites that are unknown. It prudently cautions against freeware or shareware, even though some publishers distribute legitimate software in this manner.

Note. Software required for an employee's responsibilities should be vetted by the data security coordinator, preferably in conjunction with the tax practice's IT staff or IT consultant.

Providing Personal or Business Information

Individuals must use caution when providing personal or business information. A **social engineer** attempts to acquire physical or electronic access to data by manipulating people often by using a person, website, or email. The target receives an email or call with believable information that includes names, titles, responsibilities, and other personal or business information to convince them the request is credible.

The employee code of conduct should remind employees to never respond to unsolicited calls or emails or disclose sensitive business or personal information. Additionally, employees should never provide usernames or passwords and the company should never request that information. Hackers can also use information on the type of operating system, brand of firewall, Internet browser, or which applications are installed to break into the system; employees should beware of providing that information.

Pop-Up Windows

An employee code of conduct should remind employees to watch out for pop-up windows when they are connected to the Internet. Employees should not click on pop-up windows and should use a pop-up blocker that only allows pop-up windows on trusted websites.

Password Management

An employee code of conduct should include password management for using strong passwords. Strong passwords should abide by the following protocols.

- Passwords should consist of a random sequence of at least 12 upper and lowercase letters, numbers, and special characters.
- Employees should use 2FA for systems or applications with important information.
- After acquiring new devices, employees should immediately change default administration passwords.
- Passwords should be changed at least every three months.
- Passwords protecting business information should not be reused.

Conducting Business Online Securely

Employees conducting online business, commerce, or banking should do so only on a secure browser connection. A secure browser connection is generally indicated by a small lock icon in the lower right corner or the upper left of the browser window. The code of conduct recommends employees regularly erase the web browser cache, cookies, temporary Internet files, and history, especially after using a public computer or following any online commerce or banking activities. Clearing the Internet activity prevents hackers from stealing important information if the system is compromised. Employees should look in the web browser's privacy or security menu or review the web browser's help manual for assistance.

SECURITY BREACH PROCEDURES

Despite the best intentions of a tax practice, it may still become a victim of a data breach. A compromised practice should have a response plan ready that identifies the necessary parties who should be alerted. Attachment C in Appendix A at the end of this chapter identifies the following parties that a victim should notify.

- IRS Stakeholder Liaison
- State Attorney General
- FBI, if the breach is a cybercrime that involves electronic data theft
- FTC
- Local law enforcement

- Tax software vendor
- Insurance carrier or agency

Note. If a compromised tax practice has an insurance policy under which a claim may be made, the tax practitioner should contact the agency as soon as possible. Not only is this important to establish coverage, but the insurance company may also be able to deploy a team of its employees to assist with complying with federal and state laws in notifying clients, notifying government agencies, in protecting the practice from further intrusions, and undertaking forensic investigations to determine the extent of the breach.

- Attorney
- Clients[43]

Note. Firms may also consider informing credit bureaus and any state revenue agency. Many states require businesses that collect certain data to notify affected clients and possibly the attorney general in the event of a data loss.[44] For example, under state law in Illinois, the attorney general must be notified if more than 500 Illinois residents are affected by a data breach. Tax practitioners with clients who are Illinois residents wishing to make this report or to discuss it with the attorney general's office should email **datasecurity@ilag.gov** or call 1-800-243-0618.[45] The law is relevant even for tax practitioners residing in states other than Illinois if they have more than 500 affected clients living in Illinois.

Note. The following pages on the IRS website may contain valuable information in the event of a data breach.

- **uofi.tax/23x1x1** [www.irs.gov/identitytheft]
- **uofi.tax/23x1x2** [www.irs.gov/identity-theft-fraud-scams/identity-theft-information-for-tax-professionals]
- **uofi.tax/23x1x3** [www.irs.gov/newsroom/identity-theft-information-for-businesses]

The WISP template also provides the following procedures for a firm to follow after suffering a data breach.

- Visit IRS e-Services and check an electronic filing identification number (EFIN) activity report to verify any returns filed on the practitioner's EFIN.
- Check if any questionable returns were submitted at odd hours outside normal business hours, such as overnight or on weekends.
- Scrutinize any returns transmitted on a Monday or Tuesday morning as often a thief will remotely steal the client data over the weekend when no one is in the office to notice, then rework the returns over the weekend and transmit them on a business workday after the weekend.

Note. Practitioners can find more information on security breach procedures at **uofi.tax/21x1x4** [www.irs.gov/newsroom/tax-security-101-security-summit-outlines-data-theft-reporting-process-for-tax-professionals-speed-helps-protect-taxpayers].

43. For guidance on notifying victims, see *Data Breach Response: A Guide for Business*. Feb. 2021. Federal Trade Commission. [www.ftc.gov/business-guidance/resources/data-breach-response-guide-business] Accessed on Dec. 9, 2022.

44. 815 ILCS 530/10(e)(2).

45. *Data Breach Reporting for Businesses and State Government Agencies.* Office of the Illinois Attorney General. [illinoisattorneygeneral.gov/consumer-protection/for-businesses/data-breach] Accessed on Sep. 6, 2023.

DATA ATTACKS

Client information is at a constant risk of attack, both from a cyberattack and physical compromise of data. Practitioners need to be aware of the different types of attacks to develop effective counterattacks to protect personal data.

Tax practices are vulnerable to attempted data theft because they maintain PII. To accurately prepare tax returns, tax practitioners maintain documents that verify clients' identities and their income, deductions, and credits. For a data thief, the following information is probably as valuable as the money in a bank.

- **Tax practitioner's name and contact information.**[46] A tax practitioner's name, contact information, and EFIN constitute valuable information when possessed by the wrong persons. Cybercriminals can use this information to file fraudulent tax returns. Using tools on the IRS website, a tax practitioner can monitor the use of their EFIN and PTIN. If the number of returns filed with a tax practitioner's PTIN is significantly greater than those they know they have prepared and filed, it likely indicates fraudulent use of the PTIN. [46]
- **Client personal information.** With possession of a client's personal information, criminals could file a fraudulent tax return and possibly steal money from the federal treasury.
- **Financial and employment information.** Information about a taxpayer's bank accounts, investment accounts, and employment aids a criminal in making their fraudulent attempt to impersonate a taxpayer more realistic, enabling them to pilfer the taxpayer's money, take out loans that the taxpayer is obligated to repay, or obtain a large refund by filing a fraudulent tax return in the taxpayer's name.
- **Powers of attorney.** Attorneys, EAs, and CPAs can communicate directly with the IRS regarding a client's status, provided that the IRS has on file a power of attorney (POA) or tax information authorization (TIA). Unfortunately, on rare occasions, criminals have been able to impersonate enrolled tax practitioners, enabling them to acquire taxpayers' confidential information. Aware of this threat, the IRS now validates enrolled practitioners' identities by asking callers to confirm their SSNs and dates of birth.

Practitioner Planning Tip

Tax practitioners can confirm that POAs are on file only for current clients. They may find that they still have access to former clients' records, necessitating their withdrawal from the representation of those clients.

This confirmation aims to ensure that the tax practitioner is only authorized to access records for current clients. It requires submitting a Centralized Authorization File (CAF) Client Listing Request, described on the IRS website: **uofi.tax/23x1x5** [www.irs.gov/privacy-disclosure/freedom-of-information-act-foia-guidelines]. This request is the eighth item in the list on this page, and provides a sample letter to request a listing of POAs and TIAs on file with the CAF unit of the IRS. Tax practitioners can file this request on the webpage for **FOIA.gov**, but they can also mail it to an address provided on the webpage.

46. *IRS, Summit Partners Issue Urgent EFIN Scam Alert to Tax Professionals.* Feb. 10, 2021. IRS. [www.irs.gov/newsroom/irs-summit-partners-issue-urgent-efin-scam-alert-to-tax-professionals] Accessed on Mar. 16, 2023; See *How to Maintain, Monitor and Protect Your EFIN*. Jun. 16, 2022. IRS. [www.irs.gov/tax-professionals/how-to-maintain-monitor-and-protect-your-efin] Accessed on Mar. 24, 2023.

The report showing POAs and TIAs may prove even more valuable if it includes a fraudulently filed POA, possibly indicating an individual has sought to impersonate a tax practitioner. To determine this, the tax practitioner needs to review the entire list of POAs and TIAs, looking for individuals having unfamiliar names because they have never been clients. The presence of an unfamiliar name implies someone could fraudulently impersonate the tax practitioner to obtain information on the individual with the unfamiliar name.

PHISHING ATTACKS[47]

Phishing attacks attempt to steal PII by enticing the recipient of an email into surrendering information. These attacks generally use email to initiate communication with an unsuspecting victim. The volume of emails is such that an individual message may not receive the scrutiny it needs for its recipient to discern it as fraudulent. In other cases, the fraudulent message may appear on social media or arrive by text or phone. Individuals with fraudulent intent may use phone calls in conjunction with phishing attacks to gain the confidence of unsuspecting employees, resulting in them providing passwords over the phone or surrendering other valuable information.

> **Example 14.** In 2018, the City of Batavia, Illinois, fell victim to a phishing attack that led to employee PII being released to an unknown fraudster.[48] It started when a city employee received an emailed request for Form W-2 information. The email appeared to come from the city administrator on the day that Forms W-2 had to be filed, January 31. The employee replied with the names, addresses, SSNs, and earnings of 240 city employees and city council members. Only after sending the information did the employee question the message's authenticity.
>
> The city administrator met with employees to discuss the release of PII after immediately notifying them. The city notified the local police, who investigated the incident, as well as their insurance carrier. The city provided employees with one year of credit monitoring and identity theft protection at no cost to them.

The objective of phishing attacks is not always the direct theft of PII. Phishing attacks can also attempt to install malware on computers, later subjecting them to a less detectable form of data theft.[49] The malware could be ransomware, which renders the computer inoperable.

A barrage of email messages may attempt to contact as many individuals as possible at once in the hope that one recipient, who is not careful, triggers the mechanism that installs malware or releases PII. One estimate holds that 3.4 billion phishing messages are sent **each day.**[50] Another strategy is to closely emulate an expected email message so that even a relatively cautious recipient mistakes the fraud for a legitimate email message. Because the fraudulent sender of this type of message usually is directed at specific individuals, it has earned the dubious distinction of its own name, specifically "spear phishing."[51]

---

47. *Report Phishing and Online Scams.* Jan. 20, 2023. IRS. [www.irs.gov/privacy-disclosure/report-phishing] Accessed on Mar. 16, 2023.

48. *Confidential information of Batavia city employees, elected officials stolen in phishing scam*. Girardi, Linda. Feb. 2, 2018. Aurora Beacon-News. [www.chicagotribune.com/suburbs/aurora-beacon-news/ct-abn-batavia-phishing-st-0204-20180202-story.html] Accessed on Nov. 17, 2022; *Phishing attacks: defending your organisation*. Jan. 7, 2022. National Cyber Security Centre. [www.ncsc.gov.uk/guidance/phishing] Accessed on Nov. 17, 2022.

49. *How to Recognize, Remove, and Avoid Malware*. May 2021. Federal Trade Commission. [consumer.ftc.gov/articles/how-recognize-remove-avoid-malware] Accessed on Mar. 24, 2023.

50. *How Many Phishing Emails Are Sent Daily in 2023? (New Stats).* Campbell, Stefan. Dec. 3, 2022. The Small Business Blog. [thesmallbusinessblog.net/how-many-phishing-emails-are-sent-daily] Accessed on Mar. 24, 2023.

51. *Spear phishing targets tax pros and other businesses*. Jun. 30, 2022. IRS. [www.irs.gov/newsroom/spear-phishing-targets-tax-pros-and-other-businesses] Accessed on Mar. 24, 2023.

Tax practitioners who receive messages that they believe may be phishing attempts should follow these steps.[52]

- If the message claims to be from the IRS, tax practitioners should verify it actually originated at the IRS before replying to it.
- Emails requesting information from Forms W-2 should be reported to the Internet Crime Complaint Center at **www.ic3.com**.
- If a tax practitioner falls victim to a request for PII, especially Form W-2 information, they should report this to **dataloss@irs.gov**.
- Tax practitioners should report unsolicited email messages referencing the IRS or tax matters to **phishing@irs.gov**.
- Tax practitioners should report unsolicited **fax** messages referencing the IRS both to the Treasury Inspector General for Tax Administration at **www.tigta.gov/hotline** and to the IRS at **phishing@irs.gov**.
- Suspicious phishing email messages that do not claim to be from the IRS can be forwarded to **reportphishing@antiphishing.org**.
- An individual may receive a suspicious email message which they suspect carries malware or other malicious code, but which does not claim to be from the IRS. If they have clicked on a link in the message or downloaded an attachment, they should visit **OnGuardOnline.gov**, where they can get up-to-date information from the FTC on action to be taken.

Note. The IRS takes attacks on small businesses, including tax practices, very seriously. As such, it listed phishing attacks on the Dirty Dozen list of top tax scams during 2023.[53]

SMISHING ATTACKS[54]

Some enterprising hackers have turned text messages into devices for pilfering PII, using the same strategy as phishing emails. The name smishing is a combination of "SMS" (short message service) and "phishing." Because text messages generally come from individuals one already knows, and smishing attacks are new, they receive more credibility. The IRS requests that individuals report tax-related smishing attacks to the agency via email. Individuals should send the email to **phishing@irs.gov**, including the caller ID number and email address from the incoming message, the date and time of the message, and the recipient's phone number. Although they can send it as a screenshot, the IRS prefers text information.

52. *Report Phishing and Online Scams.* Jan. 20, 2023. IRS. [www.irs.gov/privacy-disclosure/report-phishing] Accessed on Mar. 24, 2023.

53. *Dirty Dozen*. Apr. 5, 2023. IRS. [www.irs.gov/newsroom/dirty-dozen] Accessed on Jun. 1, 2023.

54. *Dirty Dozen: IRS urges tax pros and other businesses to beware of spearphishing; offers tips to avoid dangerous common scams.* Mar. 29, 2023. IRS. [www.irs.gov/newsroom/dirty-dozen-irs-urges-tax-pros-and-other-businesses-to-beware-of-spearphishing-offers-tips-to-avoid-dangerous-common-scams] Accessed on Apr. 10, 2023.

KEYLOGGERS[55]

Keyloggers intercept messages or passwords as computer users enter them on a keyboard. Modern keystroke logging is often a form of software that collects keystrokes. Sometimes this software is used in a legitimate sense, for example, when an IT department attempts to resolve issues. Other keystroke loggers are also available, which could be among the following.

- USB devices innocuously plugged into the back of a computer
- Software running on the low-level firmware of a computer or even on a nearby smartphone
- Sensors receiving electromagnetic emissions that are triggered when a typist presses specific keys on a keyboard

RANSOMWARE[56]

Ransomware removes an employee's ability to access their firm's data by covertly encrypting it and offering to decrypt it after their firm pays a ransom. Thus, users still have their proprietary data but cannot see it, interact with it, or use it because it is encrypted. This attack devastates a tax practice because it removes the firm's ability to prepare tax returns for its clients. The hackers do not have access to the firm's data but instead request untraceable funds transfers as ransom. The Treasury Department announced that the losses associated with 2021 ransomware attacks exceeded $1 billion.[57]

The federal Cybersecurity and Infrastructure Security Agency (CISA) publishes a list of Ransomware Prevention Best Practices, which may assist tax practitioners in preventing ransomware attacks on their businesses. They suggest the following actions.[58]

- Backup data, system images and configurations, keeping the backups offline
- Update and patch systems
- Ensure that security solutions are up to date
- Review and exercise (or practice) the business's incident response plan
- Pay attention to other ransomware events, applying lessons learned

Local Copy vs. Cloud Copy[59]

In the past, most small businesses used local backups, as slow Internet connection speeds did not make storing PII on the cloud practical. While this was useful, storing PII on a detachable storage device in a practitioner's possession did not protect data from a regional disaster.

---

55. *Tax Security 2.0 — A "Taxes-Security-Together" Checklist – Step* 3. Jan. 31, 2023. IRS. [www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-3] Accessed on Mar. 24, 2023; *Keystroke Logging*. Oct. 13, 2022. Wikipedia. [en.wikipedia.org/wiki/Keystroke_logging] Accessed on Nov. 17, 2022.

56. IRS Pub. 4557, *Safeguarding Taxpayer Data; Ransomware Guide.* Sep. 2020. Cybersecurity & Infrastructure Security Agency. [www.cisa.gov/stopransomware/ransomware-guide] Accessed on Nov. 17, 2022.

57. *Reported Ransomware Incidents, Costs Soared in 2021, Treasury Says*. Rundle, James. Nov. 4, 2022. Wall Street Journal. [www.wsj.com/articles/reported-ransomware-incidents-costs-soared-in-2021-treasury-says-11667513649?mod=Searchresults_pos2&page=1] Accessed on Nov. 17, 2022.

58. *CISA INSIGHTS: Ransomware Outbreak.* Aug. 21, 2019. Cybersecurity & Infrastructure Security Agency. [www.cisa.gov/uscert/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf] Accessed on Feb. 22, 2023.

59. *What is Cloud Backup? Cloud vs Local Backup Comparison*. Jan. 20, 2023. Acronis International GmbH. [acronis.com/en-us/blog/posts/cloud-vs-local-backup] Accessed on Mar. 26, 2023; See *Disaster Recovery*. Jan. 14, 2023. Wikipedia. [en.wikipedia.org/wiki/Disaster_recovery] Accessed on Mar. 26, 2023.

The preference for Internet-based (cloud) backups changed when Internet connection speed increased. It became practical to store data on remote storage in another part of the country, far removed from the same threat of regional disaster as the tax practice might face. Thus, it is now common for small tax practices to store backups of their data securely on remote devices.

However, there may be circumstances when **local** data is still preferred. If a tax practice receives a ransomware attack during tax season, it may be possible to restore data from the Internet without paying a ransom, but it potentially takes a long time. Data restoration from a local device may be the only practical means of restoring the data during tax season. Thus, tax practices may consider a network-attached storage device for local data backup. Fraudsters may encrypt PII possessed by the tax practice in a ransomware attack. In that case, restoration from a network-attached storage device stored in the server room may enable recovery from a ransomware attack within a few hours and without paying a ransom.

BRUTE FORCE ENTRY[60]

With a brute force entry attack, a hostile individual attempts to access a computer system with repeated guesses at passwords. For this reason, many systems disable logging in after a certain number of failed attempts. The hostile individual may start with simple passwords, which are subsequently modified. The user generally attempts to access the computer remotely, which enables them to use software that enters password guesses repeatedly.

The following are some characteristics of a typical victim's technical environments.

- Lacks 2FA
- Allows easy-to-guess passwords (e.g., "Taxhelp123")
- Uses inbox synchronization, which downloads email from the Internet to remote devices
- Permits users to set up email forwarding
- Limits logging, which in turn limits the investigations of any event
- Uses federated authentication, which enables access to multiple systems from a single sign-on

PHYSICAL REMOVAL[61]

Physical theft of a computer is sometimes a threat. Generally, tax practitioners can prevent physical theft of the computer system by securing the room in which the computer is stored or by securing the computer with a cable lock.

Mobile devices present a special challenge, as the very reason users carry them also makes them susceptible to physical theft. Thus, the case for encrypted hard disks is strong for laptop computers, much more than servers or other devices used only in locked locations.

INVOLVEMENT OF OUTSIDE IT SERVICES FIRMS

The WISP template and the FTC impose requirements for technical sophistication on every tax practice. Tax practitioners have all they can handle with tax law changes, let alone the rapid evolution of security threats and the computer technology they use to prepare tax returns. Thus, the involvement of outside IT specialists strengthens the long-term viability of a tax practice.

---

60. *Brute Force Attacks Conducted by Cyber Actors.* May 6, 2020. Cybersecurity & Infrastructure Security Agency. [www.cisa.gov/uscert/ncas/alerts/TA18-086A] Accessed on Nov. 17, 2022.

61. *Protecting Portable Devices: Physical Security*. McDowell, Mindi. Sep. 27, 2019. Cybersecurity & Infrastructure Security Agency. [www.cisa.gov/news-events/news/protecting-portable-devices-physical-security] Accessed on Apr. 10, 2023.

ETHICAL HACKERS[62]

An ethical hacker is an outside consultant hired by a business to probe its security weaknesses. They may attempt to access the firm's network remotely, either through a VPN or another remote access mechanism. They may test the complexity of the password attached to the firm's router. An ethical hacker helps a firm find weaknesses in its data protection.

Because many security breaches result from office personnel voluntarily providing access information or passwords, ethical hackers may use phone calls to test the resistance that office personnel offer to requests for PII. For example, an ethical hacker may call the tax practice and request that the receptionist urgently provide copies of Forms W-2 or tax returns.

NETWORK MONITORING[63]

Any server controlling a local network generates a large volume of statistics reflecting the health of the network and potential security issues. During tax season, when a tax practice is most dependent on the productivity of its employees, it may well be unreasonable to expect an employee to recognize potential issues affecting the health or even the viability of the firm. Outsourcing this function to an organization that specializes in it may prove to be the most cost-effective approach to maintaining employees' productivity and possibly averting a data breach.

INTERNET CONNECTION MONITORING[64]

In almost all cases, a router connects the tax practice's internal network to the outside world, receiving and sending data on these networks. As previously indicated, the WISP template requires that a router be "secured and maintained by the firm's IT services provider." In effect, this mandates that an outside IT firm protect PII in the tax practice's possession. Because its manufacturer must refresh a router periodically with new software and firmware, a contract with the router's manufacturer should be anticipated and perhaps budgeted.

WEBSITE FIREWALL MANAGEMENT[65]

A website for any firm is typically on an external network not directly controlled by the firm's internal network or its outside IT consultants. Nevertheless, a website can be hacked, infected with malware, or fall victim to other adverse consequences. Although some website hosting services specializing in websites for tax practices may provide management and protective functions, a website constructed by an independent designer may need its own firewall to protect the site from being taken over by malicious parties. Although it is unlikely that a tax practice would store PII on a website, tax practitioners should periodically check to ensure that no PII is accessible on the practice's website.

> **Note**. Tax practitioners can identify vendors by searching on the Internet for "website endpoint firewall" or "web application firewall."

TRAINING

An IT services firm may be able to provide training for tax practice employees on security-related matters. This training could be incorporated into the required annual training, so that employees are confident in their abilities to detect phishing messages that are probably harmful.

---

62. Baysden, Chris (Host). How to protect your CPA practice from hackers. [Audio podcast episode] In *Journal of Accountancy Podcast.* [www.journalofaccountancy.com/podcast/protect-cpa-practice-from-hackers.html] Accessed on Apr. 10, 2023.

63. *Monitoring Active Directory for Signs of Compromise*. Jun. 6, 2022. Microsoft Corp. [learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise] Accessed on Dec. 7, 2022.

64. *What is a Router?* 2022. Cisco Systems, Inc. [www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html#~how-to-choose-small-business-routers] Accessed on Dec. 7, 2022.

65. *What is a Web Application Firewall?* 2022. Cloudflare, Inc. [www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/] Accessed on Dec. 7, 2022.

DISCUSSION SCENARIOS

The following scenarios are offered to encourage tax practitioners to consider applications of the principles addressed previously.

DISCUSSION SCENARIO 1

Ken owns a small tax practice, employing two full-time, year-round tax professionals and three staff who work on a seasonal basis. Ken owns a central computer server on which his firm has loaded its network-based tax software for the past 10 years. Ken also owns document management software that stores the 1,500 tax returns the practice prepares and files annually. Ken is not considering changing tax preparation software but moving to an externally-hosted platform so that he does not have to manage the server.

What are the security considerations? _____

_____

_____

_____

Should the firm move the tax software to an externally hosted server? _____

_____

_____

_____

How should the firm implement the requirement that passwords be changed every three months? _____

_____

_____

_____

What other actions should the firm undertake to protect PII? _____

_____

_____

_____

DISCUSSION SCENARIO 2

TNY, CPA, is a small tax practice trying to wean its clients from using unsecured email to submit documents. However, the clients are not responding and continue to send PII through email, including Forms W-2.

Does TNY have liability for documents it receives from clients that the clients do not send securely? _____

_____

_____

_____

Should TNY invest in a secure email system, and if so, at what price is it no longer worth it? _____

_____

_____

_____

Are there other actions that TNY should undertake, possibly in its engagement letter or its organizer? _____

_____

_____

_____

Are there services that tax practices could use to collect clients' tax information more securely with less effort? ____

_____

_____

_____

DISCUSSION SCENARIO 3

Garcia-Jones, a medium-sized tax practice preparing 2,200 tax returns for businesses and individuals, completed its WISP in November, concluding a 6-month process that had started in May, shortly after the previous filing season ended. Although the document was completed before filing season started, the firm's management realized in early December that employees had not been trained to follow its provisions for protecting client PII.

What should the practice do with its freshly printed WISP in December?_____

_____

_____

_____

What should it do with the WISP in March? Are there training activities that the tax practice could reasonably undertake during filing season? _____

_____

_____

_____

What should it do in May? Should revisions to the WISP be discussed at the tax practice's post-filing season meetings?_

_____

_____

_____

DISCUSSION SCENARIO 4

Use the same facts as **Discussion Scenario 3.** The following July, Garcia-Jones plans to complete 600 more returns during the upcoming filing season but cannot hire competent tax professionals locally. It is confident it can hire at least three licensed tax professionals, but all live in other states, and will work remotely.

What should the firm do? _____

_____

_____

_____

What changes might be required in its WISP? _____

_____

_____

_____

What data security implications does this have? _____

_____

_____

_____

APPENDIX A — EXCERPTS FROM IRS PUB. 5708

Table of Contents

WISP - Outline

The bare essentials of a Written Information Security Plan are outlined below. Be sure you incorporate all the required elements in your plan, but scale the comprehensiveness to your firm's size and type of operation. The elements in the outline are there to provide your firm a narrower scope of purpose and define the limitations the document is meant to cover. Therefore, many elements also provide your firm with a level of basic legal protections in the event of a data breach incident. For a detailed explanation of each section, please review the detailed outline provided in this document.

I. Define the WISP objectives, purpose, and scope

II. Identify responsible individuals

- **a.** List individuals who will coordinate the security programs as well as responsible persons.
- **b.** List authorized users at your firm, their data access levels, and responsibilities.

III. Assess Risks

- **a.** Identify Risks
  - List types of information your office handles
  - List potential areas for data loss (internal and external)
  - Outline procedures to monitor and test risks

IV. Inventory Hardware

- **a.** List description and physical location of each item
- **b.** Record types of information stored or processed by each item

V. Document Safety Measures in place

- **a.** Suggested policies to include in your WISP:
  - Data collection and retention
  - Data disclosure
  - Network protection
  - User access
  - Electronic data exchange
  - Wi-Fi access
  - Remote access
  - Connected devices
  - Reportable Incidents
- **b.** Draft Employee Code of Conduct

VI. Draft an implementation clause

VII. Attachments

SAMPLE WISP TEMPLATE

Written Information Security Plan (WISP)

For

[Your Firm Name Here]

This Document is for general distribution and is available to all employees.
This Document is available to Clients by request and with consent of the Firm's Data Security Coordinator.

Last Modified/Reviewed **[Last Modified Date]**
[Should review and update at least annually]

I. OBJECTIVE

Our objective, in the development and implementation of this comprehensive **Written Information Security Plan (WISP)**, is to create effective administrative, technical, and physical safeguards for the protection of the **Personally Identifiable Information (PII)** retained by **[Your Firm Name],** (hereinafter known as **the Firm**). This WISP is to comply with obligations under the Gramm-Leach-Bliley Act and Federal Trade Commission Financial Privacy and Safeguards Rules to which the Firm is subject. The WISP sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII retained by the Firm. For purposes of this WISP, PII means information containing the first name and last name or first initial and last name of a Taxpayer, Spouse, Dependent, or Legal Guardianship person in combination with any of the following data elements retained by the Firm that relate to Clients, Business Entities, or Firm Employees:

A. Social Security number, Date of Birth, or Employment data

B. Driver's license number or state-issued identification card number

C. Income data, Tax Filing data, Retirement Plan data, Asset Ownership data, Investment data

D. Financial account number, credit or debit card number, with or without security code, access code, personal identification number; or password(s) that permit access to a client's financial accounts

E. E-mail addresses, non-listed phone numbers, residential or mobile or contact information

PII shall not include information that is obtained from publicly available sources such as a Mailing Address or Phone Directory listing; or from federal, state or local government records lawfully made available to the general public.

II. PURPOSE

The purpose of the WISP is to:

A. Ensure the Security and Confidentiality of all PII retained by the Firm.

B. Protect PII against anticipated threats or hazards to the security or integrity of such information.

C. Protect against any unauthorized access to or use of PII in a manner that creates a substantial risk of Identity Theft or Fraudulent or Harmful use.

III. SCOPE

The Scope of the WISP related to the Firm shall be limited to the following protocols:

A. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing PII.

B. Assess the potential damage of these threats, taking into consideration the sensitivity of the PII.

C. Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control identified risks.

D. Design and implement this WISP to place safeguards to minimize those risks, consistent with the requirements of the Gramm-Leach-Bliley Act, the Federal Trade Commission Financial Privacy and Safeguards Rule, and National Institute of Standards recommendations.

E. Regular monitoring and assessment of the effectiveness of aforementioned safeguards.

IV. IDENTIFIED RESPONSIBLE OFFICIALS

[The Firm] has designated [Employee's Name] to be the Data Security Coordinator (hereinafter the DSC). The DSC is the responsible official for the Firm data security processes and will implement, supervise, and maintain the WISP. Accordingly, the DSC will be responsible for the following:

- Implementing the WISP including all daily operational protocols
- Identifying all the Firm's repositories of data subject to the WISP protocols and designating them as Secured Assets with Restricted Access
- Verifying all employees have completed recurring Information Security Plan Training
- Monitoring and testing employee compliance with the plan's policies and procedures
- Evaluating the ability of any third-party service providers not directly involved with tax preparation and electronic transmission of tax returns to implement and maintain appropriate security measures for the PII to which we have permitted them access, and
- Requiring third-party service providers to implement and maintain appropriate security measures that comply with this WISP
- Reviewing the scope of the security measures in the WISP at least annually or whenever there is a material change in our business practices that affect the security or integrity of records containing PII
- Conducting an annual training session for all owners, managers, employees, and independent contractors, including temporary and contract employees who have access to PII enumerated in the elements of the WISP. All attendees at such training sessions are required to certify their attendance at the training and their familiarity with our requirements for ensuring the protection of PII. See Employee/Contractor Acknowledgement of Understanding at the end of this document

[The Firm] has designated [Employee's Name] to be the Public Information Officer (hereinafter PIO). The PIO will be the firm's designated public statement spokesperson. To prevent misunderstandings and hearsay, all outward-facing communications should be approved through this person who shall be in charge of the following:

- All client communications by phone conversation or in writing
- All statements to law enforcement agencies
- All releases to news media
- All information released to business associates, neighboring businesses, and trade associations to which the firm belongs

V. INSIDE THE FIRM RISK MITIGATION

To reduce internal risks to the security, confidentiality, and/or integrity of any retained electronic, paper, or other records containing PII, the Firm has implemented mandatory policies and procedures as follows:

PII Collection and Retention Policy

A. We will only collect the PII of clients, customers, or employees that is necessary to accomplish our legitimate business needs, while maintaining compliance with all federal, state, or local regulations.

B. Access to records containing PII is limited to employees whose duties, relevant to their job descriptions, constitute a legitimate need to access said records, and only for job-related purposes.

C. The DSC will identify and document the locations where PII may be stored on the Company premises:

- **a.** Servers, disk drives, solid-state drives, USB memory devices, removable media
- **b.** Filing cabinets, securable desk drawers, contracted document retention and storage firms
- **c.** PC Workstations, Laptop Computers, client portals, electronic Document Management
- **d.** Online (Web-based) applications, portals, and cloud software applications such as Box
- **e.** Database applications, such as Bookkeeping and Tax Software Programs
- **f.** Solid-state drives, and removable or swappable drives, and USB storage media

D. Designated written and electronic records containing PII shall be destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.

- **a.** Paper-based records shall be securely destroyed by shredding or incineration at the end of their service life.
- **b.** Electronic records shall be securely destroyed by deleting and overwriting the file directory or by reformatting the drive on which they were housed.
- **c.** Specific business record retention policies and secure data destruction policies are in an attachment to this WISP.

Personnel Accountability Policy

A. A copy of the WISP will be distributed to all current employees and to new employees on the beginning dates of their employment. It will be the employee's responsibility to acknowledge in writing, by signing the attached sheet, that he/she received a copy of the WISP and will abide by its provisions. Employees are actively encouraged to advise the DSC of any activity or operation that poses risk to the secure retention of PII. If the DSC is the source of these risks, employees should advise any other Principal or the Business Owner.

- **a.** The Firm will create and establish general Rules of Behavior and Conduct regarding policies safeguarding PII according to IRS Pub. 4557 Guidelines. **[complete and attach after reviewing supporting NISTIR 7621, NIST SP-800 18, and Pub 4557 requirements]**
- **b.** The Firm will screen the procedures prior to granting new access to PII for existing employees.
- **c.** The Firm will conduct Background Checks on new employees who will have access to retained PII.
- **d.** The Firm may require non-disclosure agreements for employees who have access to the PII of any designated client determined to have highly sensitive data or security concerns related to their account.

B. The DSC or designated authorized representative will immediately train all existing employees on the detailed provisions of the Plan. All employees will be subject to periodic reviews by the DSC to ensure compliance.

C. All employees are responsible for maintaining the privacy and integrity of the Firm's retained PII. Any paper records containing PII are to be secured appropriately when not in use. Employees may not keep files containing PII open on their desks when they are not at their desks. Any computer file stored on the company network containing PII will be password-protected and/or encrypted. Computers must be locked from access when employees are not at their desks. At the end of the workday, all files and other records containing PII will be secured by employees in a manner that is consistent with the Plan's rules for protecting the security of PII.

D. Any employee who willfully discloses PII or fails to comply with these policies will face immediate disciplinary action that includes a verbal or written warning plus other actions up to and including termination of employment.

E. Terminated employees' computer access logins and passwords will be disabled at the time of termination. Physical access to any documents or resources containing PII will be immediately discontinued. Terminated employees will be required to surrender all keys, IDs or access codes or badges, and business cards that permit access to the firm's premises or information. Terminated employees' remote electronic access to personal information will be disabled; voicemail access, e-mail access, Internet access, Tax Software download/update access, accounts and passwords will be inactivated. The DSC or designee shall maintain a highly secured master list of all lock combinations, passwords, and keys, and will determine the need for changes to be made relevant to the terminated employee's access rights.

PII Disclosure Policy

A. No PII will be disclosed without authenticating the receiving party and without securing written authorization from the individual whose PII is contained in such disclosure. Access is restricted for areas in which personal information is stored, including file rooms, filing cabinets, desks, and computers with access to retained PII. An escort will accompany all visitors while within any restricted area of stored PII data.

B. The Firm will take all possible measures to ensure that employees are trained to keep all paper and electronic records containing PII securely on premises at all times. When there is a need to bring records containing PII offsite, only the minimum information necessary will be checked out. Records taken offsite will be returned to the secure storage location as soon as possible. Under no circumstances will documents, electronic devices, or digital media containing PII be left unattended in an employee's car, home, or in any other potentially insecure location.

C. All security measures included in this WISP shall be reviewed annually, beginning **[annual calendar review date]** to ensure that the policies contained in the WISP are adequate and meet all applicable federal and state regulations. Changes may be made to the WISP at any time they are warranted. When the WISP is amended, employees will be informed in writing. The DSC and principal owners of the firm will be responsible for the review and modification of the WISP, including any security improvement recommendations from employees, security consultants, IT contractors, and regulatory sources.

D. [The Firm] shares Employee PII in the form of employment records, pension and insurance information, and other information required of any employer. The Firm may share the PII of our clients with the state and federal tax authorities, Tax Software Vendor, a bookkeeping service, a payroll service, a CPA firm, an

Enrolled Agent, legal counsel, and/or business advisors in the normal course of business for any Tax Preparation firm. Law enforcement and governmental agencies may also have customer PII shared with them in order to protect our clients or in the event of a lawfully executed subpoena. An IT support company may occasionally see PII in the course of contracted services. Access to PII by these third-party organizations will be the minimum required to conduct business. Any third-party service provider that does require access to information must be compliant with the standards contained in this WISP at a minimum. The exceptions are tax software vendors and e-Filing transmitters; and the state and federal tax authorities, which are already compliant with laws that are stricter than this WISP requires. These additional requirements are outlined in IRS Publication 1345.

Reportable Event Policy

A. If there is a Data Security Incident that requires notifications under the provisions of regulatory laws such as The Gramm-Leach-Bliley Act, there will be a mandatory post-incident review by the DSC of the events and actions taken. The DSC will determine if any changes in operations are required to improve the security of retained PII for which the Firm is responsible. Records of and changes or amendments to the Information Security Plan will be tracked and kept on file as an addendum to this WISP.

B. The DSC is responsible for maintaining any Data Theft Liability Insurance, Cyber Theft Insurance Riders, or Legal Counsel on retainer as deemed prudent and necessary by the principal ownership of the Firm.

C. The DSC will also notify the IRS Stakeholder Liaison, and state and local Law Enforcement Authorities in the event of a Data Security Incident, coordinating all actions and responses taken by the Firm. The DSC or person designated by the coordinator shall be the sole point of contact with any outside organization not related to Law Enforcement, such as news media, non-client inquiries by other local firms or businesses and other inquirers.

VI. OUTSIDE THE FIRM RISK MITIGATION

To combat external risks from outside the firm network to the security, confidentiality, and/or integrity of electronic, paper, or other records containing PII, and improving - where necessary - the effectiveness of the current safeguards for limiting such risks, the Firm has implemented the following policies and procedures.

Network Protection Policy

A. Firewall protection, operating system security patches, and all software products shall be up to date and installed on any computer that accesses, stores, or processes PII data on the Firms network. This includes any Third-Party Devices connected to the network.

B. All system security software, including anti-virus, anti-malware, and internet security, shall be up to date and installed on any computer that stores or processes PII data or the Firms network.

C. Secure user authentication protocols will be in place to:

- **a.** Control username ID, passwords and Two-Factor Authentication processes
- **b.** Restrict access to currently active user accounts
- **c.** Require strong passwords in a manner that conforms to accepted security standards (using upper- and lower-case letters, numbers, and special characters, eight or more characters in length)
- **d.** Change all passwords at least every 90 days, or more often if conditions warrant
- **e.** Unique firm related passwords must not be used on other sites; or personal passwords used for firm business. Firm passwords will be for access to Firm resources only and not mixed with personal passwords

D. All computer systems will be continually monitored for unauthorized access or unauthorized use of PII data. Event Logging will remain enabled on all systems containing PII. Review of event logs by the DSC or IT partner will be scheduled at random intervals not to exceed 90 days.

E. The Firm will maintain a firewall between the internet and the internal private network. This firewall will be secured and maintained by the Firm's IT Service Provider. The Firewall will follow firmware/software updates per vendor recommendations for security patches. Workstations will also have a software-based firewall enabled.

F. Operating System (OS) patches and security updates will be reviewed and installed continuously. The DSC will conduct a top-down security review at least every 30 days.

Firm User Access Control Policy

A. The Firm will use 2-Factor Authentication (2FA) for remote login authentication via a cell phone text message, or an app, such as Google Authenticator or Duo, to ensure only authorized devices can gain remote access to the Firm's systems.

B. All users will have unique passwords to the computer network. The firm will not have any shared passwords or accounts to our computer systems, internet access, software vendor for product downloads, and so on. The passwords can be changed by the individual without disclosure of the password(s) to the DSC or any other Firm employee at any time.

C. Passwords will be refreshed every 90 days at a minimum and more often if conditions warrant. The DSC will notify employees when accelerated password reset is necessary.

D. If a Password Utility program, such as LastPass or Password Safe, is utilized, the DSC will first confirm that:

- **a.** Username and password information is stored on a secure encrypted site.
- **b.** 2-factor authentication of the user is enabled to authenticate new devices.

Electronic Exchange of PII Policy

A. It is Firm policy that PII will not be in any unprotected format, such as e-mailed in plain text, rich text, html, or other e-mail formats unless encryption or password protection is present. Passwords MUST be communicated to the receiving party via a method other than what is used to send the data; such as by phone call or SMS text message (out of stream from the data sent).

B. The Firm may use a Password Protected Portal to exchange documents containing PII upon approval of data security protocols by the DSC.

C. MS BitLocker or similar encryption will be used on interface drives, such as a USB drive, for files containing PII.

Wi-Fi Access Policy

A. Wireless access (Wi-Fi) points or nodes, if available, will use strong encryption. Firm Wi-Fi will require a password for access. If open Wi-Fi for clients is made available (guest Wi-Fi), it will be on a different network and Wi-Fi node from the Firm's Private work-related Wi-Fi.

B. All devices with wireless capability such as printers, all-in-one copiers and printers, fax machines, and smart devices such as TVs, refrigerators, and any other devices with Smart Technology will have default factory passwords changed to Firm-assigned passwords. All default passwords will be reset or the device will be disabled from wireless capability or the device will be replaced with a non-wireless capable device.

Remote Access Policy

The DSC and the Firm's IT contractor will approve use of Remote Access utilities for the entire Firm. **Remote access is dangerous if not configured correctly and is the preferred tool of many hackers.** Remote access using tools that encrypt both the traffic and the authentication requests (ID and Password) used will be the standard. Remote Access will not be available unless the Office is staffed and systems are monitored. **Nights and Weekends are high threat periods for Remote Access Takeover data theft.** Remote access will only be allowed using 2 Factor Authentication (2FA) in addition to username and password authentication.

Connected Devices Policy

A. Any new devices that connect to the Internal Network will undergo a thorough security review before they are added to the network. The Firm will ensure the devices meet all security patch standards and login and password protocols before they are connected to the network.

B. "AutoRun" features for USB ports and optical drives like CD and DVD drives on network computers and connected devices will be disabled to prevent malicious programs from self-installing on the Firm's systems.

C. The Firm or a certified third-party vendor will erase the hard drives or memory storage devices the Firm removes from the network at the end of their respective service lives. If any memory device is unable to be erased, it will be destroyed by removing its ability to be connected to any device, or circuitry will be shorted, or it will be physically rendered unable to produce any residual data still on the storage device.

D. The firm runs approved and licensed anti-virus software, which is updated on all servers continuously. Virus and malware definition updates are also updated as they are made available. The system is tested weekly to ensure the protection is current and up to date.

Information Security Training Policy

All employees will be trained on maintaining the privacy and confidentiality of the Firm's PII. The DSC will conduct training regarding the specifics of paper record handling, electronic record handling, and Firm security procedures at least annually. All new employees will be trained before PII access is granted, and periodic reviews or refreshers will be scheduled until all employees are of the same mindset regarding Information Security. Disciplinary action may be recommended for any employee who disregards these policies.

VII. IMPLEMENTATION

Effective **[date of implementation]**, [The Firm] has created this Written Information Security Plan (WISP) in compliance with regulatory rulings regarding implementation of a written data security plan found in the Gramm-Leach-Bliley Act and the Federal Trade Commission Financial Privacy and Safeguards Rules.

Signed: _____ Date: _____

Title: [Principal Operating Officer/Owner Title]

Signed: _____ Date: _____

Title: Data Security Coordinator

SAMPLE WISP ATTACHMENTS

Attachment A: Record Retention Policies

Designated retained written and electronic records containing PII will be destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements.

It is Firm policy to retain no PII records longer than required by current regulations, practices, or standards.

I. In no case shall paper or electronic retained records containing PII be kept longer than _____ Years.

II. Paper-based records shall be securely destroyed by cross-cut shredding or incineration at the end of their service life.

III. Electronic records shall be securely destroyed by deleting and overwriting the file directory or by reformatting the drive where they were housed or destroying the drive disks rendering them inoperable if they have reached the end of their service life.

Attachment B: Rules of Behavior and Conduct Safe-guarding Client PII

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 comply with the rules of behavior. **NISTIR 7621, Small Business Information Security: The Fundamentals, Section 4**, has information regarding general rules of Behavior, such as:

- **Be careful of email attachments and web links**
    - Do not click on a link or open an attachment that you were not expecting. If it appears important, call the sender to verify they sent the email and ask them to describe what the attachment or link is. Before you click a link (in an email or on social media, instant messages, other webpages), hover over that link to see the actual web address it will take you to. Train employees to recognize phishing attempts and who to notify when one occurs.
- **Use separate personal and business computers, mobile devices, and email accounts**
    - This is especially important if other people, such as children, use personal devices. Do not conduct business or any sensitive activities (like online business banking) on a personal computer or device and do not engage in activities such as web surfing, gaming, downloading videos, etc., on business computers or devices. Do not send sensitive business information to personal email addresses.
- **Do not connect personal or untrusted storage devices or hardware into computers, mobile devices, or networks.**
    - Do not share USB drives or external hard drives between personal and business computers or devices. Do not connect any unknown/untrusted hardware into the system or network, and do not insert any unknown CD, DVD, or USB drive. Disable the “AutoRun” feature for the USB ports and optical drives like CD and DVD drives on business computers to help prevent such malicious programs from installing on the systems.
- **Be careful downloading software**
    - Do not download software from an unknown web page. Be very careful with freeware or shareware.
- **Watch out when providing personal or business information**
    - Social engineering is an attempt to obtain physical or electronic access to information by manipulating people. A very common type of attack involves a person, website, or email that pretends to be something it’s not. A social engineer will research a business to learn names, titles, responsibilities, and any personal information they can find; calls or sends an email with a believable but made-up story designed to convince you to give certain information.
    - Never respond to unsolicited phone calls that ask for sensitive personal or business information. Employees should notify their management whenever there is an attempt or request for sensitive business information.
    - Never give out usernames or passwords. No company should ask for this information for any reason. Also, beware of people asking what kind of operating system, brand of firewall, internet browser, or what applications are installed. This is information that can make it easier for a hacker to break into the system.

- **Watch for harmful pop-ups**
    - When connected to and using the Internet, do not respond to popup windows requesting that users click “OK.” Use a popup blocker and only allow popups on trusted websites.
- **Use strong passwords**
    - Good passwords consist of a random sequence of letters (upper- and lower-case), numbers, and special characters. The NIST recommends passwords be at least 12 characters long. For systems or applications that have important information, use multiple forms of identification (called “multi-factor” or “dual factor” authentication).
    - Many devices come with default administration passwords – these should be changed immediately when installing and regularly thereafter. Default passwords are easily found or known by hackers and can be used to access the device. The product manual or those who install the system should be able to show you how to change them.
    - Passwords should be changed at least every three months.
    - Passwords to devices and applications that deal with business information should not be re-used.
    - You may want to consider using a password management application to store your passwords for you.
- **Conduct online business more securely**
    - Online business/commerce/banking should only be done using a secure browser connection. This will normally be indicated by a small lock visible in the lower right corner or upper left of the web browser window.
    - Erase the web browser cache, temporary internet files, cookies, and history regularly. Ensure to erase this data after using any public computer and after any online commerce or banking session. This prevents important information from being stolen if the system is compromised. This will also help the system run faster. Typically, this is done in the web browser’s “privacy” or “security” menu. Review the web browser’s help manual for guidance.

Attachment C: Security Breach Procedures and Notifications

I. Notifications

If the Data Security Coordinator determines that PII has been stolen or lost, the Firm will notify the following entities, describing the theft or loss in detail, and work with authorities to investigate the issue and to protect the victim's identity and credit.

- The **IRS Stakeholder Liaison** who coordinates IRS divisions and other agencies regarding a Tax Professional Office data breach.
- The state Attorney General's Office
- The FBI if it is a cyber-crime involving electronic data theft
- The Federal Trade Commission, in accordance with GLB Act provisions as outlined in the Safeguards Rule.
- Local law enforcement
- Tax software vendor (can assist with next steps after a data breach incident)
- Liability insurance carrier who may provide forensic IT services
- Legal counsel
- To the extent required by regulatory laws and good business practices, the Firm will also notify the victims of the theft so that they can protect their credit and identity. The FTC provides guidance for identity theft notifications in: **Information Compromise and the Risk of Identity Theft: Guidance for Your Business**

II. Procedures

Read this **IRS Newswire Alert** for more information

Examples:

- Go to IRS e-Services and check your EFIN activity report to see if more returns have been filed on your EFIN than you transmitted.
- Check to see if you can tell if the returns in question were submitted at odd hours that are not during normal hours of operation, such as overnight or on weekends.
- Were the returns transmitted on a Monday or Tuesday morning?
    - Typically, a thief will remotely steal the client data over the weekend when no one is in the office to notice. They then rework the returns over the weekend and transmit them on a normal business workday just after the weekend.

Attachment D: Employee/Contractor Acknowledgement of Understanding

I, **[Employee Name]**, do hereby acknowledge that I have been informed of the Written Information Security Plan used by [The Firm]. I have undergone training conducted by the Data Security Coordinator. I have also been able to have all questions regarding procedures answered to my satisfaction so that I fully understand the importance of maintaining strict compliance with the purpose and intent of this WISP.

I also understand that there will be periodic updates and training if these policies and procedures change for any reason. It has been explained to me that non-compliance with the WISP policies may result in disciplinary actions up to and including termination of employment.

I understand the importance of protecting the Personally Identifiable Information of our clients, employees, and contacts, and will diligently monitor my actions, as well as the actions of others, so that [The Firm] is a safe repository for all personally sensitive data necessary for business needs.

Signed,

[Employee Name] Date: **[Date of Initial/Last Training]**

Title: **[Employee Title Description]**

Attachment E: Firm Hardware Inventory containing PII Data

Below is the enumerated list of hardware and software containing client or employee PII that will be periodically audited for compliance with this WISP.

Hardware Item	Location	Principal User	In-Service Date	Last Inventoried

Attachment F: Firm Employees Authorized to Access PII

Name	Role	Job Duties	Access Level	Date access Granted	Date Access Terminated
John Doe	DSC	Office Manager	Full access to all PII	01/01/2015	

APPENDIX B — FULL TEXT OF 16 CFR §314.4

In order to develop, implement, and maintain your information security program, you shall:

a. Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:

1. Retain responsibility for compliance with this part;

2. Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and

3. Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

b. Base your information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.

1. The risk assessment shall be written and shall include:

i. Criteria for the evaluation and categorization of identified security risks or threats you face;

ii. Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and

iii. Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

2. You shall periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks.

c. Design and implement safeguards to control the risks you identity through risk assessment, including by:

1. Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:

i. Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and

ii. Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information;

2. Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;

3. Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;

4. Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;

5. Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;

6.

i. Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and

ii. Periodically review your data retention policy to minimize the unnecessary retention of data;

7. Adopt procedures for change management; and

8. Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

d.

1. Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

2. For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:

i. Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

ii. Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

e. Implement policies and procedures to ensure that personnel are able to enact your information security program by:

1. Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

2. Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;

3. Providing information security personnel with security updates and training sufficient to address relevant security risks; and

4. Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

f. Oversee service providers, by:

1. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;

2. Requiring your service providers by contract to implement and maintain such safeguards; and

3. Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.

g. Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

h. Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas:

1. The goals of the incident response plan;

2. The internal processes for responding to a security event;

3. The definition of clear roles, responsibilities, and levels of decision-making authority;

4. External and internal communications and information sharing;

5. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

6. Documentation and reporting regarding security events and related incident response activities; and

7. The evaluation and revision as necessary of the incident response plan following a security event.

i. Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:

1. The overall status of the information security program and your compliance with this part; and

2. Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.