# Creating a Written Information Security Plan for your Tax & Accounting Practice

**Revision Date: August 2, 2022**

# Table of Contents

# Creating a Written Information Security Plan (WISP) for your Tax & Accounting Practice

This document was prepared by the Security Summit, a partnership of the Internal Revenue Service, state tax agencies, private-sector tax groups as well as tax professionals. The mission of the Security Summit is to fight identity theft and tax refund fraud.

This document is intended to provide sample information and to help tax professionals, particularly smaller practices, develop a Written Information Security Plan or WISP. It is not an exhaustive discussion of everything related to **WISPs and it is not intended to replace your own research, to create reliance or serve as a substitute for developing your own plan based upon the specific needs and requirements of your business or firm.** A written information security plan is just one part of what tax professionals need to protect their clients and themselves. Given the rapidly evolving nature of threats, the Summit also strongly encourages tax professionals to consult with technical experts to help with security issues and safeguard their systems.

There are many aspects to running a successful business in the tax preparation industry, including reviewing tax law changes, learning software updates, and managing and training staff. Creating a Written Information Security Plan or WISP is an often overlooked but critical component. Not only is a WISP essential for your business and a good business practice, the law requires you to have one. For many tax professionals, knowing where to start when developing a WISP is difficult. This guide provides multiple considerations necessary to create a security plan to protect your business, and your clients and comply with the law.

## Requirements

The Gramm-Leach-Bliley Act (GLBA) is a U.S. law that requires financial institutions to protect customer data. In its implementation of the GLBA, the Federal Trade Commission (FTC) issued the Safeguards Rule to outline measures that are required to be in place to keep customer data safe. One requirement of the Safeguards Rule is implementing a WISP.

Under the GLBA, tax and accounting professionals are considered financial institutions, regardless of size. Financial institutions subject to the Safeguards Rule include mortgage brokers, real estate appraisers, universities, nonbank lenders, and check cashing businesses.

As a part of the plan, the FTC requires each firm to:

- 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 your 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

# Getting Started on your WISP

Before you begin writing your WISP, take time to familiarize yourself with compliance requirements and your professional responsibilities. Some good resources to review before beginning include:

- IRS Publication 4557
- FTC Data Breach Response Guide

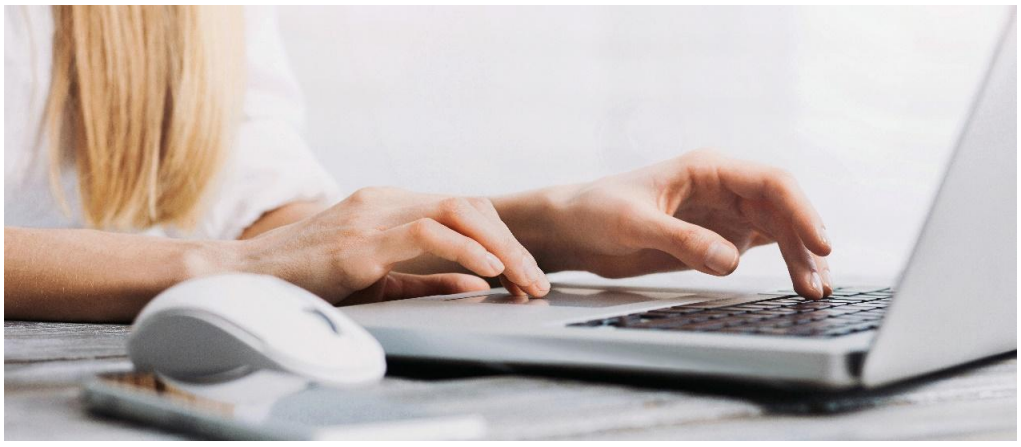
A security plan should be appropriate to the company's size, scope of activities, complexity, and the sensitivity of the customer data it handles. There is no one-size-fits-all WISP. For example, a sole practitioner can use a more abbreviated and simplified plan than a 10-partner accounting firm. A good WISP should focus on three areas:

- Employee management and training
- Information systems
- Detecting and managing system failures

It is a good idea to create an Employee/Contractor Acknowledgment of Understanding document for all personnel to keep a record of training and understanding of the policies in your WISP. Signing and dating training leaves a good documentation trail you can keep on file for several reasons – to show your adherence to the spirit of compliance and to have an enforceable accountability point in the event of a negligent employee. It is recommended that these acknowledgments be updated at annual training intervals and kept on file.

Once completed, keep your WISP in a format that others can easily read, such as PDF or Word. Making your WISP available to employees for training purposes is encouraged. Storing a copy offsite or in the cloud is a recommended best practice in the event of a physical disaster.

It is important to understand that a WISP is intended to be an evergreen document that is regularly reviewed and updated along with changes to the size, scope, and complexity of your business.



# 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 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]**

# Written Information Security Plan (WISP)

## 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**

# Added Detail for Consideration When Creating your WISP

Use this additional detail as you develop your written security plan. Review the description of each outline item and consider the examples as you write your unique plan.

## Define the WISP objectives, purpose, and scope

**Objective Statement:** This defines the reason for the plan, stating any legal obligations such as compliance with the provisions of GLBA and sets the tone and defines the reasoning behind the plan. The Objective Statement should explain why the Firm developed the plan. It also serves to set the boundaries for what the document should address and why.

**Purpose Statement:** The Purpose Statement should explain **what** and **how** taxpayer information is being protected with the security process and procedures.

**Scope Statement:** The scope statement sets the **limits** on the **intent** and purpose of the WISP. Since you should not be legally held to a standard that was unforeseen at the writing or periodic updating of your WISP, you should set reasonable limits that the scope is intended to define.

## Identify responsible individuals

Identify by name and position persons responsible for overseeing your security programs. Explain who will act in the roles of Data Security Coordinator (DSC) and Public Information Officer (PIO). In most firms of two or more practitioners, these should be different individuals. These roles will have concurrent duties in the event of a data security incident. Be sure to define the duties of each responsible individual.

- The Data Security Coordinator is the person tasked with the information security process, from securing the data while remediating the security weaknesses to training all firm personnel in security measures.
- The Public Information Officer is the “one voice” that speaks for the firm for client notifications and outward statements to third parties, such as local law enforcement agencies, news media, and local associates and businesses inquiring about their own risks.

## Assess Risks

- Identify Risks: While building your WISP, take a close look at your business to identify risks of unauthorized access, use, or disclosure of information. Carefully consider your firm's vulnerabilities.
- List types of information your office handles. Identifying the information your practice handles is a critical step in evaluating risk. Some types of information you may use in your firm includes taxpayer PII, employee records, and private business financial information. For example, do you handle paper and electronic documentation containing client or employee PII? List all types.
- List all potential types of loss (internal and external). Evaluate types of loss that could occur, including unauthorized access and disclosure and loss of access. Be sure to include any potential threats and vulnerabilities, such as theft, destruction, or accidental disclosure. Examples might include physical theft of paper or electronic files, electronic data theft due to Remote Access Takeover of your computer network, and loss due to fire, hurricane, tornado or other natural cause.
- Outline procedures to monitor your processes and test for new risks that may arise.

## Inventory Hardware

- It is imperative to catalog all devices used in your practice that come in contact with taxpayer data. This could be anything from a computer, network devices, cell phones, printers, to modems and routers.
    - List description and physical location of each item
    - Record types of information stored or processed by each item

  **Example:**

    - Jane Doe Business Cell Phone, located with Jane Doe, processes emails from clients
    - John Doe PC, located in John's office linked to the firms' network, processes tax returns, emails, company financial information.
    - Network Router, located in the back storage room and is linked to office internet, processes all types of information

      **Sample Attachment E - Firm Hardware Inventory containing PII Data**

## Document Safety Measures

- This section sets the policies and business procedures the firm undertakes to secure all PII in the Firm's custody of clients, employees, contractors, governing any privacy-controlled physical (hard copy) data, electronic data, and handling by firm employees.

  List policies for the following:

  - Data collection and retention
    - Precisely define the minimal amount of PII the firm will collect and store
    - Define who shall have access to the stored PII data
    - Define where the PII data will be stored and in what formats
    - Designate when and which documents are to be destroyed and securely deleted after they have met their data retention life cycle
- **Data disclosure**
    - You should define any receiving party authentication process for PII received
    - Define how data containing PII will be secured while checked out of designated PII secure storage area
    - Determine any policies for the internet service provider, cloud hosting provider, and other services connected to any stored PII of the firm, such as 2 Factor Authentication requirements and compatibility
    - Spell out whom the Firm may share stored PII data with, in the ordinary course of business, and any requirements that these related businesses and agencies are compliant with the Firm's privacy standards
- **Network protection (List how your system and devices are protected)**
    - Firewall protection

- All security software, anti-virus, anti-malware, anti-tracker, and similar protections
- Secure user protocols
    - User IDs
    - Restricted access by job role
    - Password selection policy
    - Password controls to ensure no passwords are shared
    - Password change interval policy
    - Restriction on using firm passwords for personal use, and personal passwords for firm use
- Monitoring all computer systems for unauthorized access via event logs and routine event review
- Operating System patch and update policies by authorized personnel to ensure uniform security updates on all workstations

- **User access (How users access devices)**

    - Will your firm implement an Unsuccessful Login lockout procedure?
    - Two-Factor Authentication Policy controls
    - Determine any unique Individual user password policy
    - Approval and usage guidelines for any third-party password utility program

- **Remote access (How employees access data remotely)**

    - Set policy requiring 2FA for remote access connections.
    - Consider a no after-business-hours remote access policy. Historically, this is prime time for hackers, since the local networks they are hacking are not being monitored by employee users.

- **Connected devices (How new devices or software is added to the network)**

    - New network devices, computers, and servers must clear a security review for compatibility/configuration
    - Configure access ports like USB ports to disable “autorun” features
    - Set policy on firm-approved anti-virus, anti-malware, and anti-tracking programs and require their use on every connected device.
    - Require any new software applications to be approved for use on the Firm’s network by the DSC or IT Professional prior to installation.

- **Reportable Incidents**

    *Create both an Incident Response Plan & a Breach Notification Plan*

    In the event of an incident, the presence of both a Response and a Notification Plan in your WISP reduces the unknowns of how to respond and should outline the necessary steps that each designated official must take to both address the issue and notify the required parties.

    - At a minimum, plans should include what steps will be taken to re-secure your devices, data, passwords, networks and who will carry out these actions

- Describe how the Firm Data Security Coordinator (DSC) will notify anyone assisting with a reportable data breach requiring remediation procedures
- Describe who will be responsible for maintaining any data theft liability insurance, Cyber Theft Rider policies, and legal counsel retainer if appropriate
- Describe the DSC duties to notify outside agencies, such as the IRS Stakeholder Liaison, Federal Trade Commission, State Attorney General, FBI local field office if a cybercrime, and local law enforcement agencies

- **Draft Employee Code of Conduct**

  Determine a personnel accountability policy including training guidelines for all employees and contractors, guidelines for behavior, and employee screening and background checks. Address any necessary non-disclosure agreements and privacy guidelines. Be sure to include information for terminated and separated employees, such as scrubbing access and passwords and ending physical access to your business.

## Draft an Implementation Clause

When all appropriate policies and procedures have been identified and included in your plan, it is time for the final steps and implementation of your WISP. An Implementation clause should show the following elements:

- Date of implementation
- Firm Name
- That the plan is emplaced in compliance with the requirements of the GLBA
- That the plan is in compliance with the Federal Trade Commission Financial Privacy and Safeguards Rule
- Also add if additional state regulatory requirements apply
- The plan should be signed by the principal operating officer or owner, and the DSC and dated the date of implementation.

## Ancillary Attachments

Attach any ancillary procedures as attachments. These are the specific task procedures that support firm policies, or business operation rules. For example, a separate Records Retention Policy makes sense. If regulatory records retention standards change, you update the attached procedure, not the entire WISP. Other potential attachments are Rules of Behavior and Conduct Safeguarding Client PII, as recommended in Pub 4557. Another good attachment would be a Security Breach Notifications Procedure.

### Sample Attachment A - Record Retention Policy

Determine the firm's procedures on storing records containing any PII.

- How long will you keep historical data records, different firms have different standards? There are some Federal and state guidelines for records retention periods.
- How will you destroy records once they age out of the retention period?
  - How will paper records are to be stored and destroyed at the end of their service life
  - How will electronic records be stored, backed up, or destroyed at the end of their service life

***Best Practice:*** *Keeping records longer than the minimum record retention period can put clients at some additional risk for deeper audits. By common discovery rules, if the records are there, they can be audited back as far as the statutes of limitations will allow. Promptly destroying old records at the minimum required timeframe will limit any audit or other legal inquiry into your clients' records to that time frame only.*

## Sample Attachment B - Rules of Behavior and Conduct Safeguarding Client PII

Having some rules of conduct in writing is a very good idea. It standardizes the way you handle and process information for everyone in the firm. This attachment can be reproduced and posted in the breakroom, at desks, and as a guide for new hires and temporary employees to follow as they get oriented to safe data handling procedures. These sample guidelines are loosely based on the National Institute of Standards guidelines and have been customized to fit the context of a Tax & Accounting Firm's daily operations.

***Best Practice:*** *At the beginning of a new tax season cycle, this addendum would make good material for a monthly security staff meeting. Keeping security practices top of mind is of great importance. Other monthly topics could include how phishing emails work, phone call grooming by a bad actor, etc. SANS.ORG has great resources for security topics. The Ouch! Newsletter can be used as topical material for your Security meetings.*

## Sample Attachment C - Security Breach Procedures and Notifications

It is a good idea to have a guideline to follow in the immediate aftermath of a data breach. To be prepared for the eventuality, you must have a procedural guide to follow. This attachment will need to be updated annually for accuracy. Subscribing to IRS e-news and topics like the Protect Your Clients, Protect Yourselves series will inform you of changes as fraud prevention procedures mature over time.

## Sample Attachment D - Employee/Contractor Acknowledgement of Understanding

It is a good idea to have a signed acknowledgment of understanding. This is particularly true when you hire new or temporary employees, and when you bring a vendor partner into your business circle, such as your IT Pro, cleaning service, or copier servicing company. They need to know you handle sensitive personal data and you take the protection of that data very seriously.

***Best Practice:*** *It is important that employees see the owners and managers put themselves under the same rules as everyone else. When you roll out your WISP, placing the signed copies in a collection box on the office manager's desk for a time for anyone to see, for example, is a good way for everyone to see that all employees are accountable. Placing the Owners and Data Security Coordinator's signed copy on the top of the stack prominently shows you will play no favorites and are all pledging to the same standard of conduct. This acknowledgement process should be refreshed annually after an annual meeting discussing the Written Information Security Plan and any operational changes made from the prior year.*

## Sample Attachment E - Firm Hardware Inventory containing PII Data

Keeping track of data is a challenge. A good way to make sure you know where everything is and when it was put in service or taken out of service is recommended. This is especially true of electronic data.

- Include paper records by listing filing cabinets, dated archive storage boxes, and any alternate locations of storage that may be off premises.
- List all desktop computers, laptops, and business-related cell phones which may contain client PII.
- List storage devices, removable hard drives, cloud storage, or USB memory sticks containing client PII.

***Best Practice:*** *Set a policy that no client PII can be stored on any personal employee devices such as personal (not firm owned) memory sticks, home computers, and cell phones that are not under the direct control of the*

*firm. This ensures all devices meet the security standards of the firm, such as having any auto-run features turned off, and they are standardized for virus and malware scans.*

## Sample Attachment F - Firm Employees Authorized to Access PII

Having a list of employees and vendors, such as your IT Pro, who are authorized to handle client PII is a good idea. You should not allow someone who may not fully understand the seriousness of the secure environment your firm operates in to access privacy-controlled information. Additionally, an authorized access list is a good place to start the process of removing access rights when a person retires or leaves the firm. Having a systematic process for closing down user rights is just as important as granting them.

- List name, job role, duties, access level, date access granted, and date access Terminated
- Be sure to include contractors, such as your IT professionals, hosting vendors, and cleaning and housekeeping, who have access to any stored PII in your safekeeping, physical or electronic.
- List any other data access criteria you wish to track in the event of any legal or law enforcement request due to a data breach inquiry. **Examples:**
    - John Smith - Office Manager / Day-to-Day Operations / Access all digital and paper-based data / Granted January 2, 2018
    - Jane Robinson - Senior Tax Partner / Tax Planning and Preparation / Access all digital and paper-based data / Granted December 01, 2015
    - Jill Johnson - Receptionist / Phones/Scheduling / Access ABC scheduling software / Granted January 10, 2020 / Terminated December 31, 2020
    - Jill Johnson - Tax Preparer / 1040 Tax Preparation / Access all digital and paper-based data / Granted January 2, 2021

***Best Practice:*** *If a person has their rights increased or decreased It is a good idea to terminate the old access rights on one line, and then add a new entry for the new access rights granted. This shows a good chain of custody for rights and shows a progression. For the same reason, it is a good idea to show a person who goes into semi-retirement and has less rights than before and the date the status changed.*

# Sample 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.

# Sample Attachment B: Rules of Behavior and Conduct Safeguarding 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.

# Sample 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.

# Sample 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]**

# Sample 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 |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Sample 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 | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# Reference A. The Glossary of Terms

**Anti-virus software** - software designed to detect and potentially eliminate viruses before damaging the system. Can also repair or quarantine files that have already been infected by virus activity.

**Attachment** - a file that has been added to an email. It could be something useful to you, or something harmful to your computer.

**Authentication** - confirms the correctness of the claimed identity of an individual user, machine, software component or any other entity.

**Breach** - unauthorized access of a computer or network, usually through the electronic gathering of login credentials of an approved user on the system.

**Clear desk Policy** - a policy that directs all personnel to clear their desks at the end of each working day, and file everything appropriately. Desks should be cleared of all documents and papers, including the contents of the "in" and "out" trays - not simply for cleanliness, but also to ensure that sensitive papers and documents are not exposed to unauthorized persons outside of working hours.

**Clear screen Policy** - a policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentiality. Typically, the easiest means of compliance is to use a screensaver that engages either on request or after a specified brief period.

**Cybersecurity** - the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.

**Data Security Coordinator (DSC)** - the firm-designated employee who will act as the chief data security officer for the firm. The DSC is responsible for all aspects of your firm's data security posture, especially as it relates to the PII of any client or employee the firm possesses in the course of normal business operations.

**Data breach** - an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

**Encryption** - a data security technique used to protect information from unauthorized inspection or alteration. Information is encoded so that it appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using a decryption key.

**Firewall** - a hardware or software link in a network that inspects all data packets coming and going from a computer, permitting only those that are authorized to reach the other side. It is helpful in controlling external access to a computer or network.

**GLBA** - Gramm-Leach-Bliley Act. Administered by the Federal Trade Commission. Establishes safeguards for all privacy-controlled information through business segment Safeguards Rule enforced business practices.

**Hardware firewall** - a dedicated computer configured to exclusively provide firewall services between another computer or network and the internet or other external connections.

**Malware** - (malicious software) any computer program designed to infiltrate, damage or disable computers.

**Network** - two or more computers that are grouped together to share information, software, and hardware. Can be a local office network or an internet-connection based network.

**Out-of-stream** - usually relates to the forwarding of a password for a file via a different mode of communication separate from the protected file. *Example: Password protected file was emailed, the password was relayed to the recipient via text message, outside of the same stream of information from the protected file.*

**Patch** - a small security update released by a software manufacturer to fix bugs in existing programs.

**Phishing email** - broad term for email scams that appear legitimate for the purpose of tricking the recipient into sharing sensitive information or installing malware.

**PII** - Personally Identifiable Information. The name, address, SSN, banking or other information used to establish official business. Also known as Privacy-Controlled Information.

**Public Information Officer (PIO)** - the PIO is the single point of contact for any outward communications from the firm related to a data breach incident where PII has been exposed to an unauthorized party. This position allows the firm to communicate to affected clients, media, or local businesses and associates in a controlled manner while allowing the Data Security Coordinator freedom to work on remediation internally.

**Risk analysis** - a process by which frequency and magnitude of IT risk scenarios are estimated; the initial steps of risk management; analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats.

**Security awareness** - the extent to which every employee with access to confidential information understands their responsibility to protect the physical and information assets of the organization.

**Service providers** - any business service provider contracted with for services, such as janitorial services, IT Professionals, and document destruction services employed by the firm who may come in contact with sensitive client PII.

**Software firewall** - an application installed on an existing operating system that adds firewall services to the existing programs and services on the system.

**VPN (Virtual Private Network)** - a secure remote network or Internet connection encrypting communications between a local device and a remote trusted device or service that prevents en-route interception of data.

**Written Information Security Plan** - a documented, structured approach identifying related activities and procedures that maintain a security awareness culture and to formulate security posture guidelines. Mandated for Tax & Accounting firms through the FTC Safeguards Rule supporting the Gramm-Leach-Bliley Act privacy law.

# Resource Links:

Below are helpful links from within the WISP creation guide above and also from outside sources like the Federal Communications Commission (FCC), and the National Institute of Standards and Technology (NIST). These resources in addition to IRS and Federal Trade Commission resources will support your efforts to create a durable Written Information Security Plan for your firm.

### Federal Trade Commission

- FTC Financial Institution How to Comply
- FTC Safeguards Rule
- FTC Data Breach Response Guide

### National Institute of Standards

- Cybercrime & Cyber Threats to Small Business
  - Cybercrime its worse we thought
  - Cybercrime existential threat small business
- NIST Computer Security Resource Center
- NIST Cybersecurity Framework examples

### Federal Communications Commission

- FCC Cyber Threat Resources

### Internal Revenue Service

- IRS Publication 4557
- IRS Stakeholder Liaison
- IRS Data Theft Reporting Process