Written Information Security Plan (WISP)

For

Company Name

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 Reviewed:

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 Company 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. 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

Company Name has designated Name of DSC 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.

Company Name has designated Name of PIO 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 Appendix A.

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. 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. See Appendix B at the end of this document.
    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 to 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 Insert 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. Company Name 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, 9an 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. See Appendix C at the end of this document.

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 improve - 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 Firm's 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 Firm's network. A list of Firm software can be found in Appendix D.
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 every 365 days, or under specific conditions, such as user requests or when there is evidence of a compromise.
    e. 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 adhere to Federal Trade Commission 15 U.S.C § 6805. Section 314.4(c.5) regarding the implementation of multi-factor authentication.
B. The Firm will use multi-factor authentication (MFA) 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.
C. All users will have unique passwords to the computer network. The Firm will not have any shared passwords or accounts for our computer systems, internet access, software vendor for product downloads, etc. Passwords can be changed by the user without disclosure of the password to the DSC or any Firm employee at any time.
D. Passwords will be refreshed in accordance with the National Institute of Standards and Technology (NIST) guidelines. The DSC will notify employees when accelerated password reset is necessary.

E. 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. Multi-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 multi-factor Authentication (MFA) 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. Information Security and Phishing training is being provided by external vendor, Watch Cloud Cyber Security. Disciplinary action may be recommended for any employee who disregards these policies.

VII. IMPLEMENTATION

Effective Insert Date, Company Name 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: _____

APPENDIX 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.

A. In no case shall paper or electronic retained records containing PII be kept longer than 3 Years.
B. Paper-based records shall be securely destroyed by cross-cut shredding or incineration at the end of their service life.
C. 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.

APPENDIX 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.
    - NIST guidelines recommend password reset every 365 days, or when a compromise has occurred.
    - 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.

APPENDIX 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.

a. The IRS Stakeholder Liaison who coordinates IRS divisions and other agencies regarding a Tax Professional Office data breach.
b. The state Attorney General's Office
c. State tax agencies - Visit the Federal Tax Administrators' "Report a Breach" for state-by-state information.
d. The FBI's Internet Crime Complaint Center if it is a cyber-crime involving electronic data theft.
e. The Federal Trade Commission, in accordance with GLB Act provisions as outlined in the Safeguards Rule. Report security events affecting 500 or more people within 30 days of discovery through the FTC's online Safeguards Rule Security Event Reporting Form.
f. Local law enforcement
g. Tax software vendor (can assist with next steps after a data breach incident)
h. Liability insurance carrier who may provide forensic IT services.
i. Legal counsel
j. 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

a. 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.
b. Check to see if the returns in question were submitted at odd hours that are not during normal hours of operation, such as overnight or on weekends.
c. Consult Data theft information for tax professionals | Internal Revenue Service

APPENDIX D: Current Business & Security Related Software

Security Services	Function	Vendor
Anti-Virus	Detects, blocks, and removes malicious software from your system	
EDR	Monitors, detects, and responds to threats on endpoints in real-time	
MDR	Provides 24/7 threat detection, analysis, and response by experts	
VPN	Encrypts internet traffic and hides your IP for secure browsing	
Backup	Copies and stores data to restore after loss or damage	
Drive Encryption	Protects data by converting it into unreadable code without a key	
WISP Management	Create and update WISP	
Phishing Education	Trains staff to recognize and avoid fraudulent phishing attacks	
Phishing Simulation	Tests employee response to fake phishing attacks to improve awareness	
Data Theft Recovery Management	Prepares and guides your firm's response to recover stolen data	
Firewall	Blocks unauthorized access to your network and sensitive client data	