Written Information Security Plan (WISP)
for
Legacy Tax & Accounting Solutions, LLC

Formerly Implemented October 25, 2022
To be reviewed each October
Last revised November 14, 2024

This Document is for general distribution and is available to all employees.
This Document is also posted on the website at kinzeycpa.com

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 the Legacy Tax & Accounting Solutions, LLC, (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. The staff are trained to treat all client documents and information as PII when safeguarding & handling data as a Best policy rather than have the staff try to determine what items should be safeguarded. By treating all data we come in contact with as PII, then more security is provided. The exception is if PII is provided by the client to us via email as those emails typically will not be deleted.

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 Scott K. Kinzey, CPA, MTax 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

The Firm has designated Scott K. Kinzey, CPA, MTax 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.

We use the cloud-based software called Tax Canopy for document management and storage. All staff has access to all clients. Birthdays are not maintained in Tax Canopy.

We also use the cloud-based Thomson Reuters Ultra Tax software for all tax return preparation. Only tax preparers in the Firm have access year-round to this software.

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

a. No PII is kept on local servers, disk drives, solid-state drives, USB memory devices or removable media

b. No PII is kept in physical filing cabinets or securable desk drawers.

c. PII is kept in the contracted document retention companies Tax Canopy and Thomson Reuters Ultra Tax.

d. No PII is kept on PC Workstations, OneDrive or Laptop Computers.

e. PII is kept in client portals and electronic Document Management software known as Tax Canopy as explained above.

f. Cloud-based accounting software known as QuickBooks On-line for applications for Bookkeeping.

g. PII is kept in the cloud-based software hosted by Right Networks to keep only QuickBooks Desktop version. Each client data file is password protected.

h. No PII is kept on solid-state drives, and removable or swappable drives, and USB storage media

i. Staff have ability to use an app on their cell phones or tablets to access data in Canopy but such access requires a facial recognition multi-factor authentication.

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 at the end of their service life. The typical project holds these items for less than 30 days as the project is completed.

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. See the Risk area below for business record retention policies and secure data destruction policies.

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 screen the procedures prior to granting new access to PII for existing employees.

b. The Firm will conduct Background Checks on new employees who will have access to retained PII.

B. 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. Currently the Firm has strict oral policies of non-disclosure of PII.

C. The DSC orally or by e-mail reminds employees from time to time of various items in this WISP.

D. All employees are responsible for maintaining the privacy and integrity of the Firm's retained PII.

E. 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.

F. 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.

PII Disclosure Policy

The entire WISP will be listed on the website under its own page.

A. No PII will be disclosed without authenticating the receiving party and without securing authorization from the individual whose PII is contained in such disclosure.

B. All security measures included in this WISP shall be reviewed annually, beginning 2022 but the annual review will be done in the fall of each year 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.

C. 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. 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.

Risk area items (items to work out moving forward)

The following items listed are acknowledged that more work needs to be done in order to pin these items down or resolve them.

1. There is no current policy on record retention nor time tables for client destruction of data. With digital data storage almost free, the need to destroy data seems almost irrelevant. There are legal reasons that could prohibit keeping data that needs to be explored. For lost clients, the data is backed up and stored digitally.

2. Scott to obtain from these four third party cloud-based software companies their PII policies: Tax Canopy, Thompson Reuters Ultra Tax, Splashtop and Right Networks.

3. 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]

4. The Firm size is small and all current employees have been reminded and informed about the use of PII and related issues. It is being considered to conduct 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. Also being considered is that 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 following the *Employee/Contractor Acknowledgement of Understanding* document.

5. Since no PII is maintained on local PCs, it is contemplated that a physical (i.e. hardware) firewall is not needed. That said, it will be explored moving into the future and possibly include this: 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.

6. Since PII is not kept on local PC's, then using MS BitLocker or similar encryption on interface drives, such as a USB drive, for files containing PII seems irrelevant.

7. Not yet sure how this applies: 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.

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. Current insurance carrier is Hartford policy and State Farm.

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.

D. 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 (https://www.irs.gov/businesses/small-businesses-self-employed/stakeholder-liaison-local-contacts) who coordinates IRS divisions and other agencies regarding a Tax Professional Office data breach.

  Submit Form 14039-B to the IRS for identity theft.

Arizona – Area 5	203-492-8630	CL.SL.Area.5@irs.gov
Missouri – Area 6	206-946-3703	CL.SL.Area.6@irs.gov

- State level agencies stateAlert@taxadmin.org

  Arizona 602-716-6300

  Missouri 573-751-3505 idtheft@dor.mo.gov

- The state Attorney General's Office. Arizona 602-542-5025. Missouri 573-290-5679.

- The FBI if it is a cyber-crime involving electronic data theft. This is known as the IC-3 Department that can retrieve ACH money stolen as this department can freeze checking accounts in the US banking system SWIFT. Internet Crime Center (IC-3) a division of the FBI 202-324-3000 or file written report at www.ic3.gov
- The Federal Trade Commission, in accordance with GLB Act provisions as outlined in the Safeguards Rule.
- Local law enforcement to file a police report to establish the event. Cottonwood police 928-634-4246.
- Tax software vendor (can assist with next steps after a data breach incident) Thomson Reuters Ultra Tax 800-968-0600.
- Document management and portal vendor Tax Canopy 855-616-7305.
- Liability insurance carrier who may provide forensic IT services. Agent for Hartford Insurance David Goldstein 928-567-0335; Agent for State Farm Insurance Katie Clouse 417-581-1600.
- Legal counsel. Natalia Garrett 602-703-5225.
- 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".*

- *Ben@resolveITComputers.com is a Springfield vendor that is knowledgeable in this area.*
- *Scott has attended classes on this topic: National Association of Tax Professionals 9-8-22; Missouri Society of Accountants 9-23-24.*

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. Keep in mind that no PII is maintained on the local network.

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. The digital Firewall is Defender by Microsoft. No physical firewall is employed as all PII is kept in cloud-based third party software.

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, ten or more characters in length)
   d. Change all passwords at least every 90 days. Thomson Reuters forces this implementation which is the reminder that the DSC sends to all employees to change their passwords as well.

D. 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.

E. 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.

This is being employed for Tax Canopy, Thomson Reuters Ultra Tax, QuickBooks On-line and Right Networks.

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.

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. Currently PII is shared only via the portal inside Tax Canopy.

Wi-Fi Access Policy

A. All firm PC's and printers, even those at a remote employee location, are strictly barred from using Wireless access (Wi-Fi). Only wired connections are allowed. Wi-Fi for clients is made available (guest Wi-Fi) and it is considered on a "different network" as none of the PC's are on the Wi-Fi.

Remote Access Policy

The DSC 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. The Firm uses the cloud-based third party provider "Splashtop" for one employee to work remote when not in the office. **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. "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. Upon connecting any flash drive to a local PC, a Defender scan is run.

B. The DSC will physically destroy (i.e. a hammer to the hard drive) the hard drives or memory storage devices the Firm removes from service at the end of their respective service lives.
C. 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 informed from time to time on maintaining the privacy and confidentiality of the Firm's PII. The DSC will provide guidance on the specifics of paper record handling, electronic record handling, and Firm security procedures from time to time but 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 October 25, 2022, Kinzey CPA 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: Scott K. Kinzey 10-25-22
Title: Principal owner Date
Scott K. Kinzey, CPA, MTax

Signed: Scott K. Kinzey 10-25-22
Title: Data Security Coordinator (DSC) Date
Scott K. Kinzey, CPA, MTax

Glossary of Terms provided by the Internal Revenue Service

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.