a

rightworks

Written Information Security Plan (WISP)

PREPARED FOR

{{CompanyName}}

{{StreetAddress1}}

{{EmailAddress}}

{{PrepPerson}}

Created on: {{Date}}

Annual Review Date: {{AnnualReviewDate}}

I. OBJECTIVE

The objective of {{CompanyName}}'s **(the "Company")** WISP is to support and document the implementation and maintenance of necessary protective measures the Company has selected to protect the personally identifiable information (PII) and other sensitive customer data it collects, creates, uses and maintains. This WISP has been prepared in line with the requirements and guidelines of the IRS, the Gramm-Leach-Bliley Act (GLBA), and the FTC Safeguards Rule. This document will also act as the comprehensive record of all internal policies and processes designed to secure information of Company's customers.

II. PURPOSE

- Ensure the proper security and confidentiality of PII and other sensitive customer information collected, created and maintained.
- Comply with applicable data security laws; including IRS Publication 4557, 5708 and the FTC Safeguards Rule.
- Document and show auditors/ data safeguards and policies.
- Define an information security program that is appropriate to the Company's size, business and resources, and the amount of PII and other sensitive information maintained by the Company.
- Protect clients from unauthorized access.

III. SCOPE

- Applies to all employees, contractors, officers and directors of the Company.
- Applies to any PII storage locations or records.
- Applies to security of PII and sensitive information of both the company and its clients.
- Cataloging existing preventive strategies against data breaches.
- Ongoing evaluation and review of the efficacy of the established protective measures.
- For the purposes of this WISP, PII includes any of the following items to the extent it could be used, alone or in combination with other information, to identify a specific natural person or individual household:

PII includes

- First and last name combination
- Personal phone number
- Purchase history
- Bank account information
- Credit card numbers
- CRM data
- Tax prep software data
- Driver's license information
- Social security number
- Date of birth
- Employment history

- Previous tax returns
- Financial statements
- Private email addresses

Checklist: Required FTC Software and Policies

	Description	Citation	Place/ Not In Place	Vendor/Date
□	Designate a qualified individual	16 CFR 314.4 (a)	In Place	
□	Conduct risk assessment	16 CFR 314.4 (a)	In Place	
□	Encryption at rest	16 CFR 314.4 (c) (3)	In Place	
□	Encryption in transit	16 CFR 314.4 (c) (3)	In Place	Rightworks
□	Multifactor authentication	16 CFR 314.4 (c) (5)	In Place	Choose an item.
□	Continuous monitoring with IDS/RMM or network scan and penetration testing	16 CFR 314.4 (d) (2)	Choose an item.	Choose an item.
□	Security awareness training	16 CFR 314.4 (e)	Choose an item.	Choose an item.
□	Date: Assess providers	16 CFR 314.4 (f)	Choose an item.	
□	Date: Annual WISP review	16 CFR 314.4 (g)	Choose an item.	
□	Develop a Written Information Security Plan	16 CFR 314.4 (h)	Choose an item.	
□	Date: Annual director reports	16 CFR 314.4 (h)	Choose an item.	
□	Date: Annual disposal of records	FTC SWS (1)	Choose an item.	
□	Restricted access to data	FTC SWS (2)	Choose an item.	
□	Require complex passwords	FTC SWS (3)	Choose an item.	
□	Firewall	FTC SWS (5)	Choose an item.	Choose an item.
□	Intrusion detection systems (IDS)	FTC SWS (5)	Choose an item.	Choose an item.

□	Segmented / IOT / Guest network	FTC SWS (5)	Choose an item.	
□	Endpoint security	FTC SWS (6)	Click here to enter text.	Choose an item.
□	Third-party patch management	FTC SWS (6)	Choose an item.	Choose an item.
□	Windows patch management	FTC SWS (6)	Choose an item.	Choose an item.

Checklist: IRS “Security Six”

Use an antivirus	
Choose an item.	Antivirus installed: Choose an item.
Choose an item.	Endpoint detection and response: Choose an item.
Choose an item.	Intrusion detection systems: Choose an item.

Use a firewall	
Choose an item.	Firewall: Choose an item.

Multifactor authentication	
Choose an item.	Accessing customer data: Choose an item.

Use backup software/services	
Choose an item.	Backup: Choose an item.
Choose an item.	Is it encrypted?

Use drive encryption	
Choose an item.	Encryption through: Choose an item.

Create and secure virtual private networks	
Choose an item.	VPN: Choose an item.

IRS Publication 4557: Safeguarding Taxpayer Data

Create strong passwords	
Choose an item.	Enforce password history: 24 (max) passwords remembered
Choose an item.	Minimum of 8 characters
Choose an item.	Password must meet complexity requirements: Enabled
Choose an item.	Avoid personal information use phrases instead
Choose an item.	Change default/temporary passwords that come with accounts including printers
Choose an item.	Store passwords in a secure location like a safe or locked file cabinet
Choose an item.	Use MFA for password manager

Secure wireless networks	
Choose an item.	Default login on router?
Choose an item.	Turn off public SSID
Choose an item.	Change guest wireless network to unidentifiable name
Choose an item.	Reduce WLAN Transmit power (TX) range to not work outside of office if needed
Choose an item.	WPA2 and AES Encryption enabled
Choose an item.	Do not use WEP

Protect stored client data	
Choose an item.	Disallow installing unnecessary software or applications
Choose an item.	Perform an inventory of devices containing client data

Choose an item.	Limit / disable access to stored client data

Proactive safety	
Choose an item.	RMM: Choose an item.
Choose an item.	Patch management on browsers? Choose an item.
Choose an item.	Disable stored password feature offered by some operating systems

Create a data security plan	
Choose an item.	Printed and readily available?
Choose an item.	Point of contact established **{{FirstName}} {{LastName}}**
Choose an item.	Incident response plan in place in case of breach
Choose an item.	Security and awareness training: Choose an item.

PII inventory list

List anywhere that contains PII. Examples include but are not limited to:

1. Third-party apps

a. ______________________________

b. ______________________________

2. Cloud provider(s)

a. ______________________________

b. ______________________________

3. Data storage(s)

a. ______________________________

b. ______________________________

4. Email provider(s)

a. ______________________________

b. ______________________________

5. CRM(s)

a. ____

b. ____

6. Social media contractor(s)

a. ____

b. ____

Qualified Individual implementing and supervising the information security program

Qualified Individual: _______________________________________

Qualifications/experience: _______________________________________

Supervisor: _______________________________________

Company's Qualified Individual shall report in writing to the Company's [Board of Directors] [senior management] and such report shall include an overall assessment of Company's compliance with the information security program and provide specific reporting on the elements provided in this Written Information Security Plan, as well as security events and how management responded, and recommendations for changes in the information security program.

Risk assessment

The Company will periodically conduct risk assessments in light of changes to its operations or the emergence of new threats to determine foreseeable risks and threats, both internal and external, to the security, confidentiality and integrity of customer information. This risk assessment will take into account the customer information collected, used, stored, and otherwise processed by the Company. The risk assessment findings will be memorialized in a report and will include the criteria used for evaluating the risks and threats, taking into account how customer information could be disclosed without authorization, misused, altered, or destroyed.

Security program safeguards

Access controls: Company has implemented and periodically review access controls in a manner designed to ensure that those who have access to customer information have a legitimate business need for it.

Data inventory: Company has conducted, and will periodically conduct, an inventory of customer information to maintain an accurate list of all systems, devices, platforms, and personnel that collect, host, store or otherwise process customer information. Company shall use this inventory to inform its periodic risk assessments and related security controls.

Encryption: Company encrypts customer information at rest and in transit. Any deviation from this requirement requires written approval from the Company's Qualified Individual and a description of the effective alternative controls provided to that specific use case.

Application assessments: All Company-owned or third party application used to collect, host, store, or otherwise process customer information shall be assessed on a periodic basis in a manner designed to determine whether such applications provide appropriate security for such customer information and, where appropriate, Company shall implement compensating safeguards as approved by the Qualified Individual on the basis of such assessments.

Multifactor authentication: Company has implemented and shall maintain multifactor authentication solutions for all users accessing customer information that is collected, hosted, stored or otherwise processed by the Company. For the purposes of this Written Information Security Plan, multifactor authentication shall require at least two of the following three authentication factors: a knowledge factor (for example, a password); a possession factor (for example, a token); and an inherence factor (for example, biometric characteristics). Any deviation from this requirement requires written approval from the Company's Qualified Individual and a description of the effective alternative controls provided to that specific use case.

Secure disposal: Company shall securely dispose of customer information no later than two years after Company's most recent use of it to serve the customer, unless such customer information elements are required to be retain by Company pursuant to a legitimate business need or legal requirement to hold on to it or if targeted disposal isn't feasible because of the way the information is maintained. For example, copies of tax returns prepared by the Company will generally be retained for seven years. Any deviation from this requirement requires written approval from the Company's Qualified Individual and a description of the effective alternative controls provided to that specific use case.

Change management: Company has processes in place to evaluate changes to its information system, network, or other collection, hosting, storage or processing of Customer Information designed to identify whether the existing security controls are appropriate or require updates. Company shall engage in appropriate penetration and vulnerability testing in response to material changes to operations or business arrangements, or as otherwise may be appropriate in response to changes within the Company or its operations.

Logging and monitoring: Company maintains a log of authorized users' activity and has implemented alerting solution to identify unauthorized access to its information systems or network. Company has implemented and maintains procedures and controls to monitor when authorized users are accessing customer information and to detect unauthorized access.

Service providers: Company shall engage service providers with appropriate capabilities to maintain appropriate safeguards for customer information, impose on such service providers contractual provisions regarding customer information security, auditing and/or monitoring of the service provider, and conduct period re-assessments of service providers for suitability from a security standpoint.

Incident response: Company has implemented and maintains a written information security plan that provides:

- A statement of the purposes and goals of the response plan;
- The internal processes activated in response to a security event;
- Clear roles, responsibilities, and levels of decision-making authority;
- Communication channels for information sharing internally and externally;
- A process to remediate any identified weaknesses in Company systems and controls;
- Procedures for documenting and reporting security events and the response; and the response; and
- A process to engaged in a postmortem review and remediation.

Testing: Company conducts:

- annual penetration testing;
- periodic vulnerability assessments;
- system-wide scans every six months designed to test for publicly-known security vulnerabilities; and
- penetration and vulnerability testing in response to material changes as provided in the section on Change Management.

Training: Company shall provide employees and other authorized users accessing customer information on its behalf with this Written Information Security Plan, associated policies and procedures, and regular and role-appropriate security awareness training and require notification to the Qualified Individual of any potential security risks or threats to customer information.

APPENDIX:

Additional information security policies and procedures

As part of this WISP, the Company will develop, maintain and distribute information security policies and procedures to relevant employees, contractors and other stakeholders.

Below are sample policies/procedures to consider. Please review and customize these so they are suited for your business and include in your internal employee handbook or IT guidelines or distribute separately.

Digital document safety measures

{{CompanyName}} adopts a comprehensive cybersecurity policy focusing on the protection of Personally Identifiable Information (PII). We take efforts to only collect essential PII, ensuring minimal data exposure. We employ robust data encryption techniques to safeguard information both in transit and at rest. Access to sensitive data is controlled, limited to staff members who require it for their role, and is continuously monitored to prevent unauthorized access. To further enhance security, we use software-dependent formats for data processing, ensuring compatibility and security through regular updates. Our policy mandates the prompt disposal of files that are no longer needed (in accordance with applicable laws and other obligations), thereby reducing potential data breach risks. This includes the shredding of physical materials containing sensitive information. Multifactor authentication (MFA) is mandatory for all systems access, providing an additional layer of security. We maintain secure backups of all data, ensuring business continuity in case of unforeseen events. Regular audits are conducted to assess and improve our security measures, and we implement rigorous version control practices to track and manage data efficiently. Finally, we enforce full encryption on all drives and storage devices to secure data against unauthorized access.

Use security software

See security assessment.

Strong passwords policy

{{CompanyName}}'s password policy, aligned with cybersecurity standards, is designed to ensure strong protection for sensitive data. Our policy mandates a minimum password length of eight characters, incorporating a mix of capital letters, lowercase letters, numbers, and symbols to enhance security. Employees are instructed not to reuse passwords across different platforms or services. Personal information is to be avoided in password creation, reducing the risk of password deduction through social engineering. We encourage the use of phrases, rather than single words, to increase password complexity. All default or temporary passwords must be promptly changed upon first use. To avoid potential security breaches, employees are advised not to use their email as their username. Passwords are securely stored in a password manager, ensuring they are both strong and retrievable only by the authorized user. Password sharing is prohibited. Finally, Multi-Factor Authentication (MFA) is required on all platforms where it's available, adding an additional layer of security beyond the password itself. This comprehensive password policy forms a critical part of our overall cybersecurity strategy at **{{CompanyName}}**, safeguarding our data and systems effectively.

Secure wireless networks policy

Our wireless network security policy is designed to safeguard our network and data integrity. We begin by changing the default admin passwords on all network devices, a critical step in preventing unauthorized access. The range of our Wireless Local Area Network (WLAN) is minimized to ensure it covers only the necessary areas, reducing the risk of outside intrusion. We rename our Service Set Identifier (SSID) to something non-descriptive, making it less identifiable and thus more secure. The public visibility of our SSID is disabled, adding an extra layer of obscurity. For encryption, we exclusively use WPA2-AES, the most secure protocol, while avoiding the outdated and vulnerable WEP standard. When readily available & economically feasible, we will upgrade our network to use WPA3. Our policy dictates the use of Virtual Private Networks (VPNs) for all remote access, ensuring data is encrypted and secure when transmitted over the internet. Regular firmware updates are mandated to address any security vulnerabilities and enhance network performance. Our guest network is isolated from the main network, ensuring that visitors cannot access internal resources. Finally, we continuously monitor network activity to detect and respond to any unusual behavior or potential threats promptly. This comprehensive approach to wireless network security at **{{CompanyName}}** is integral to maintaining the confidentiality, integrity, and availability of our data and systems.

Protect stored client data policy

{{CompanyName}}'s policy for protecting stored client data is centered around robust security measures and best practices. We will utilize drive encryption, ensuring that all data stored on our drives is secured against unauthorized access. In addition to local encryption, we maintain encrypted backups of all data, safeguarding against data loss due to system failures or cyber-attacks. We employ a gapped cloud backup strategy, which involves keeping a secure, offline copy of our data in the cloud, providing an extra layer of protection. The use of public USB drives is strictly prohibited to prevent the risk of malware infections and data leaks unless from an approved device. Our policy limits the installation of extra software on devices that store client data, reducing the attack surface for potential cybersecurity threats. Inventory of all storage devices containing PII is maintained, allowing us to have complete visibility and control over where and how client data is stored. Before disposing of any data storage devices, we ensure all data is securely deleted to prevent any possibility of data recovery. Physical drives are destroyed when they are no longer in use or are being replaced, ensuring that data cannot be recovered even from discarded hardware. Multi-factor authentication is mandatory, when available, for accessing any system that stores client data, adding an additional layer of security beyond just passwords. For added security, certain critical data is stored off-site in secure storage facilities, protecting it from local physical threats.

Spot data theft

All employees and contractors have been trained in the most common ways to spot data theft and breaches within our systems. This includes vigilance against multiple types of anomalies and suspicious activities. Our system is designed to detect if there are any duplicate Social Security Number filings. We pay close attention to unexpected IRS letters or instances where refunds are issued to clients who have not filed their taxes, as these can indicate fraudulent activities. Alerts from the IRS accounts and mismatches in the Electronic Filing Identification Number (EFIN) count are closely monitored to ensure the integrity of our filing process. Furthermore, our system is equipped to identify subtle signs of a breach, such as clients reaching out in regards to messages we never sent. On the user level, lockouts, software login errors, and unusual file changes are tracked. We also keep an eye on mismatched forms, random pop-ups, and the presence of unknown devices on our network, from unauthorized access attempts. Lastly, repeated failed login attempts are logged and investigated, as they can often be the precursor to a more severe security breach. Security Awareness Training is also conducted through: **{{SecurityAwarenessMethod}}**

Monitoring and protecting EFIN

To ensure the security and proper use of our Electronic Filing Identification Number (EFIN), it is imperative to implement a consistent monitoring process, particularly during the peak of the filing season. This is a critical period when the risk of unauthorized use of EFINs is heightened. Regular monitoring can be efficiently achieved through the EFIN Status page, an exclusive section on the IRS website designed for this purpose. This page provides us with the exact count of tax returns the IRS has attributed to any EFIN. By routinely comparing these official figures with internal records, we can promptly identify any discrepancies or unusual activities. The data on the EFIN Status page is updated weekly, ensuring we have access to the most recent information. This frequency is particularly beneficial during the busy tax season when volumes are high, and any misuse of our EFIN can have significant repercussions. In the event we discover a discrepancy, such as a notably higher volume of returns filed under any Company EFIN than what has been recorded, immediate action is required in accordance with our incident response plan, including coordination with legal counsel, and contacting the IRS e-help Desk at 866-255-0654. Furthermore, this proactive monitoring approach is not just about responding to potential threats; it is also a preventive measure. By keeping a close eye on Company EFIN activity, the Company can deter potential bad actors and maintain the integrity of the Company's filing process. The Company provides education to its internal team about the importance of EFIN security. Regular training sessions and updates on security protocols can go a long way in ensuring that everyone understands the role they play in safeguarding this critical asset. By monitoring the EFIN via the IRS' status page, we are not only complying with IRS regulations but also protecting our clients and practice from potential fraud and other forms of financial crime.

Guard against phishing scams

In our effort to fortify our organization against phishing scams, we have implemented a multi-layered approach that encompasses various strategies and tools. A key aspect of this policy is the separation of personal and business email accounts. This distinction ensures that professional communications are less susceptible to phishing attempts that often target personal inboxes. To enhance the security of our email communication, we have mandated the use of two-factor authentication (2FA) for all business email accounts. We recognize the importance of maintaining clean systems, and as such, regular scans for malware are conducted on all devices. Employees are advised to be cautious about opening attachments from unknown sources, as these can often be vehicles for malware or phishing attempts. In line with this, any suspicious emails purporting to be from the IRS or similar entities are to be immediately forwarded to our internal security team for verification. Spam filters are activated on all our email accounts where possible / economically feasible to reduce the likelihood of phishing emails reaching our inboxes. We also ensure that only verified plugins are used within our systems to prevent security breaches through third-party software. Employees are trained to check URLs before clicking on links to avoid falling victim to phishing attempts that mimic legitimate websites. We also emphasize the importance of confirming the identity of email senders, especially in communications involving sensitive information. Regular updates of all software, including email clients, browsers, and security tools, are mandatory to protect against vulnerabilities that could be exploited in phishing attacks.

Be safe on the internet

Effective management of software updates is a crucial component of our cybersecurity strategy, particularly concerning web browsers and operating systems. To ensure that all third-party software remains up to date with the latest security patches, we understand it is recommended to utilize a robust third-party patch management tool. Alongside the third-party tools, we elect to have Windows patched and updated regularly. This ensures that our systems are protected against vulnerabilities that are commonly addressed in these regular updates. Our policy is to apply patches following "Patch Tuesday" as a guide. Patches will be applied and rebooted no more than 72 hours after the patch has been released. In addition to these measures, we have a policy of scanning all downloaded files before opening them. This is a critical step in preventing malware infections that can be embedded in seemingly harmless downloads. We implement a monthly tune up process on all endpoint machines and servers. These tune-ups include software updates, hardware checks, and optimization tasks to ensure peak performance and security of our systems. Removal of temporary internet files, cookies, and browsing history where applicable. When traveling, all employees are to use a VPN to secure connection when using unfamiliar WiFi. When browsing online, we emphasize the importance of looking for the 'HTTPS://' protocol in the website URL, which signifies a secure connection. This simple check can significantly reduce the risk of data interception and other cyber threats. Lastly, our security protocol dictates that employees should never use the 'Remember Password' feature in web browsers. While convenient, this practice can pose a significant security risk, especially if a device falls into the wrong hands.

Service providers

Vetting service providers thoroughly is crucial to ensure they align with our security standards. This vetting process should include defining clear security expectations to which these providers must adhere. Additionally, incorporating security monitoring clauses within service agreements enables ongoing oversight of a service provider's security practices. Periodic reassessments of the service providers are scheduled to maintain a high level of security compliance. These reassessments are complemented by conducting background checks on all relevant personnel, ensuring that those with access to sensitive information are trustworthy. It is also mandated that service providers hold relevant security certifications, reflecting their commitment and competence in handling data securely. Upon selecting service providers, we will ask for references from actual customers to see their real-world experience with the provider to see if their stated commitment to security is in alignment with what clients' receive. We also insist on auditing our service providers regularly to verify their compliance with our security expectations. In the case of any security incidents, our service provider agreements shall require providers to report these incidents to the Company promptly.

Multifactor authentication policy

Our policy requires the use of strong passwords in combination with multifactor authentication (MFA) for all users. This approach reduces the risk of unauthorized access, ensuring that even if a password is compromised, the additional layer of security provided by MFA acts as a barrier from unwanted access. The Company requires all passwords to be changed immediately upon the termination of employment of an employee or the termination of a contractor relationship in order to maintain the integrity of our systems. To combat the threat of brute force attacks, we employ long, complex passwords along with the requirement of MFA for all accounts. Our security measures include full encryption of all hard drives. This encryption ensures that any data on the devices remains secure and inaccessible to unauthorized individuals. Furthermore, we store all sensitive financial information in the cloud, where it is protected by advanced security measures. This approach not only safeguards the data in case of physical theft but also allows for better control and monitoring of access to this sensitive information.

Employee management and training

Every new employee must sign a confidentiality agreement upon joining the Company. This agreement binds them to our strict standards for safeguarding customer information. Access to sensitive customer data is restricted to only those employees who require it for their specific job functions, such as customer service representatives, and is limited to the extent necessary for completing their tasks. Employees are regularly trained to adhere to all Company guidelines on information security to maintain the confidentiality and integrity of customer information. Employees are trained to report any suspicious attempts to obtain customer information to designated personnel. Regular reminders about the Company's security policies and legal obligations to keep customer data confidential are communicated to employees. This is reinforced with visible reminders in areas where sensitive information is stored. For remote workers, specific telecommuting policies are in place, detailing how customer data can be accessed or stored at home.

Detecting and managing system failures

Prevention with a proactive approach to cybersecurity, we will be updating our security programs on a regular basis. Some of these updates will be done automatically through software designed to implement patch management. The software will be chosen by a third-party IT provider that will regularly install patches from third-party software vendors, alongside consistent updates of Windows patches, to safeguard against vulnerabilities. Our managed firewall will be another basis of security in the firm. Closing any unused ports to prevent unauthorized access. Standard ports shall remain open at the suggestion of our managed IT provider and with reasonable explanation, we shall approve/deny their requests. The firm also prioritizes rapid communication with employees regarding any security issues, ensuring that all team members are informed and vigilant. Security awareness training is a key aspect to preventing intrusions into the system. The use of intrusion detection systems plays a critical role in detecting potential breaches early, allowing for quick response and mitigation. Finally, the implementation of a dummy account within our Software as a Service (SaaS) systems serves as an additional layer of security. This strategy is designed to detect unauthorized access and provide insights into potential vulnerabilities within our systems. We shall utilize these in a discretionary manner, mainly focusing on the areas that would potentially have the greatest impact from a breach. By adopting these comprehensive measures, the firm demonstrates its commitment to robust security practices, ensuring the protection of PII and other sensitive client data.

Policy: Safeguarding client PII for employees and contractors

The purpose of this policy is to define the required conduct and behaviors for the secure handling of client personally identifiable information (PII) in both digital and physical forms. It is mandatory for all users of our information systems to thoroughly understand, sign, and comply with these guidelines. Regarding email and web links, you must exercise caution with unexpected email attachments or links. You agree to verify the legitimacy of emails by directly contacting the sender and to hover over links to check their destination URLs. In terms of device segregation, you must maintain separate devices for personal and professional use. You must avoid conducting business-sensitive tasks on personal devices and to refrain from engaging in non-work activities like gaming or video streaming on work devices. For storage media, you should not insert personal or unknown storage devices into work computers or networks. You should disable the "AutoRun" feature for USB and optical drives to prevent the unauthorized installation of software. When it comes to software downloads, you will download software only from reputable sources and exercise caution with freeware and shareware. You should always be vigilant and wary of social engineering attempts that aim to manipulate you into revealing information about the Company or our customers. You agree to report any solicitation for sensitive information to your supervisors and never disclose usernames, passwords, or technical specifications of the system. You will ignore prompts from pop-up ads, employ a pop-up blocker, and only allow pop-ups from trusted sites. You will always comply with the Company's password policy by using the required level of complex passwords (including the usage of pass phrases over single words). You will use secure browser connections (HTTPS) for online business transactions. You will avoid using public computers for business activities. You recognize that adherence to these guidelines is crucial for compliance with best practices in safeguarding client PII.

Employee / contractor name: ____

Date: ______________________________

PII data retention and destruction policy for accountants (GAAP-compliant)

This policy is established with the objective of aligning with Generally Accepted Accounting Principles (GAAP) and governing the secure handling of personally identifiable information (PII) in both paper and electronic formats. It provides clear guidelines on the retention period and secure destruction procedures for such records, ensuring compliance with legal requirements and industry best practices.

Under the data retention section of this policy, it is mandated that PII data must be retained for a period that is consistent with both business needs, GAAP requirements and other applicable laws. As a general rule, the Company shall securely dispose of customer information no later than **two** years after our most recent use of it to serve a customer, unless such information is required to be retained by Company pursuant to a legitimate business need or legal requirement. Tax returns, however, will generally be retained for **seven** years following IRS guidelines. Beyond any applicable retention periods, or if PII files are deemed unnecessary for business purposes, they should be promptly deleted.

For the destruction of paper-based records, this policy specifies secure destruction methods to be employed once these records reach the end of their required retention time. Using a shredder will be the method of physical document destruction.

Regarding the destruction of electronic records, the policy outlines specific methods to securely destroy electronic-based PII records at the end of their service life. These methods include overwriting the file directory, reformatting the storage drive, and physically destroying the drive disks to render them completely inoperable. This ensures that the data cannot be recovered or misused.

Adherence to this policy is crucial for maintaining compliance with GAAP standards and for upholding the integrity and confidentiality of PII data. It reflects the organization's commitment to responsible data management and protection of sensitive information.

Employee and contractor agreement to protect PII

I acknowledge that I have been fully briefed on the Written Information Security Plan (WISP) employed by **{{CompanyName}}**. My orientation included an in-depth training session led by the “Qualified Individual” responsible for Data Security within the organization. This session provided an open forum for addressing any questions or concerns I had, thereby ensuring my complete understanding of how vital it is to strictly adhere to the guidelines set forth in the WISP.

I am aware that this plan is not static; it will evolve and be updated periodically to address new security concerns and procedural modifications. I commit to attending any future training sessions and updates to keep abreast of these changes. I understand that my failure to comply with the WISP's policies and guidelines may result in disciplinary actions up to and including termination of my employment or engagement with **{{CompanyName}}**.

I know the critical role I play in maintaining the security of Personally Identifiable Information (PII) and other sensitive customer information that we maintain. This extends to the sensitive data belonging to our clients, fellow employees, and business contacts. I understand that **{{CompanyName}}** serves as a custodian for this data and it is paramount that I act diligently to preserve its integrity and security. I also acknowledge my responsibility to be vigilant not only about my own activities but also to monitor the actions of my colleagues. My intent is to ensure that **{{CompanyName}}** maintains its reputation as a secure and trustworthy repository for any data that is essential for our business operations.

I hereby affirm my understanding and commitment to the principles outlined in this acknowledgment. I acknowledge and understand the significance of complying with the WISP and will uphold these important security measures.

Employee / contractor name: ____

Date: ______________________________

Incident Response Plan (IRP)

1. **Purpose:** The purpose of this Incident Response Plan is to provide a framework and process for all information security incidents that affect any of [[Company]]'s information technology ("IT") systems, network, or data, including [[Company]]'s data held or IT services provided by third-party vendors or other service providers (a "security incident"). This IRP shall:

a. Define our cyber incident response process and provide a step-by-step guideline for a timely and repeatable incident response process;

b. Document the appropriate third parties to contact and collaborate with in responding swiftly and responsibly to incidents; and

c. Assist our organization with mitigating the negative effects of a security incident on our organization, employees, customers and others.

2. **Scope:** This IRP applies to all [[Company]] employees, contractors, officers, and directors. A "security incident" refers to an actual or reasonably suspected (a) loss or theft of confidential, personal or sensitive information; (b) unauthorized disclosure, access to, or processing of confidential, personal or sensitive information, or (c) unauthorized access to, use of, or malicious infection of our systems or third-party systems that may compromise the privacy or confidentiality of confidential, personal or sensitive information or our operating environment.

3. **Responsible person:** [[Company]] has designated [[Title/Person]] to implement and maintain this IRP (the "Incident Coordinator"). To the extent necessary and appropriate, the Incident Coordinator will establish an Incident Response Team that will help implement the various elements of this IRP. If an Incident Response Team is established, the team members and contact information will be included in this IRP. The Incident Coordinator will also do the following:

a. Lead all post-mortem activities analyzing effectiveness of responses to security incidents and compliance with this IRP;

b. Lead any required trainings for employees to be informed of and ready to act on the requirements of this IRP; and

c. Review and revise this IRP at least annually.

4. **Enforcement:** Violations of this IRP may result in disciplinary action, up to and including termination of employment (for employees) any contractual engagement (for contractors).

5. **Internal process:** The Company shall implement the following procedures to respond to and document any security incidents:

a. The Company shall establish and maintain procedures to identify whether a security incident has occurred. Following the identification of a security incident, the Incident Coordinator shall assess the level of risk associated with such security incident, including with respect to the relative likelihood and impact of data loss, operational risks, etc.

b. The Incident Coordinator, in conjunction with the Incident Response Team, if applicable, Company management and the "Security Experts" identified below, shall determine how many disclosures and contacts to other listed entities and service providers need to occur in light of the circumstances of a particular security incident.

In the event of a security incident

	Name	Role	Contact information
Incident coordinator			
Incident risk team member			
Incident risk team member [[if applicable]]			
Incident risk team member [[if applicable]]			
Incident risk team member [[if applicable]]			

1) Initial investigation: Coordinate investigation and risk assessment of potential security incident in coordination with the Incident Response Team, if applicable, and Company management.
2) Contact security experts:
   a) **{{TechCompany}} - {{TechCompanyPhone}}** to identify the cause of the breach and how to remediate.
   b) Legal counsel – [[Counsel Name]]; [[Counsel Phone Number]]
3) Insurance company
   a) Check to see if the policy covers breach mitigation expenses.
   b) [[Insurance Broker Name and Contact Information]]
   c) [[Insurance Policy; Contact Information]]
4) Contact the IRS to inform them of the breach via phone and email.
5) Contact credit / ID theft protection agency. Certain states require offering credit monitoring / ID theft protection to victims of ID theft.
   a) Equifax: (800) 997-2493
   b) Experian: (888) 397-3742
   c) TransUnion (800) 680-7289
6) Contact FBI:
   a) Contact closest FBI Field Office.
   b) Determine disclosure process with law enforcement.
7) Contact affected customers:
   a) Send individual letters to all victims and inform them of breach.
   b) Consider your state's specific disclosure laws.
   c) Request affected customers fill out Form 14039 (Identity Theft Affidavit).

Final instructions

The “Qualified individual” (designated above) as well as any other relevant stakeholders have reviewed and modified this WISP so that it is an accurate reflection of [[Company]]’s information security program, policies and procedures.

[[Company]] will review this WISP and the security measures presented in this WISP at least annually.

Print a copy and keep on file at your business.

Next review due before: **{{ExpirationDate}}**

If you need assistance with your WISP or IT solutions: https://rightworks.com

Call: (877) 572.6989

Qualified individual

Signature: ______________________________

Date: ________________________________

Contact us

Call: +1 888.210.0237

Thank you

https://www.rightworks.com/