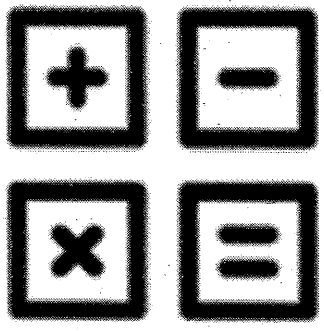
WRITTEN INFORMATION SECURITY PLAN (WISP) – 2024-25

Created On: December 1, 2024
Expires: December 1, 2025

PREPARED FOR
Stephanie Denman, EA
Tax & Bookkeeping Service
1012 S Stapley Dr. Ste. 114, Mesa, AZ 85204
admin@stephaniedenmanea.com

Prepared By: Stephanie Denman, EA



I. OBJECTIVE

The aim of Stephanie Denman, EA's WISP is to establish and record the necessary protective measures in line with the IRS, Gramm-Leach-Bliley Act (GLBA), and FTC Safeguards Rules. This document will also act as the comprehensive record of all internal policies and processes designed to secure our clients' Personally Identifiable Information (PII).

PII Includes

- First & Last Name Combination
- Personal Phone Number
- Purchase History
- Bank Account Information
- Credit Card Numbers
- CRM Data
- Tax Prep Software Data
- Driver License
- Social Security Number
- Date of Birth
- Employment History
- Previous Tax Returns
- Financial Statements
- Private Email Addresses

General rule of thumb being "can you Google this?" If the answer is no, then the data should be considered PII to protect. PII does not encompass data sourced from public directories like mailing addresses or phone listings, nor does it include information from federal, state, or local government records that are legally accessible to the public.

II. PURPOSE

- Showcase proper security.
- Comply with applicable data security laws.
- Document and show auditors/ data safeguards and policies.
- Demonstrate how we can reasonably protect PII
- Protect clients from unauthorized access

III. SCOPE

- Identifying PII storage locations and addressing security gaps, along with steps for breach prevention.
- Evaluating the impact and repercussions of a breach on 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.
- Complying with policies and procedures listed within IRS Publication 4557, 5708, and the FTC Safeguards Rule

Taxes-Security-Together
IRS Security Six Checklist

Use an Antivirus	
Pass / Fail	Antivirus Installed
Pass / Fail	Anti Spyware Installed
Pass / Fail	Anti Phishing Toolbar
Pass / Fail	Endpoint Detection & Response
Pass / Fail	Intrusion Detection Systems

Pass / Fail	Firewall

Pass / Fail	Windows / Login password protected
Pass / Fail	Accessing Customer Data

Pass / Fail	Backup
Pass / Fail	Is it Encrypted? Yes

Pass / Fail	Encryption Through

Pass / Fail	VPN

IRS Publication 4557:
Safeguarding Taxpayer Data

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

Pass / Fail	Default login on router?
Pass / Fail	Turn off public SSID
Pass / Fail	Change guest wireless network to unidentifiable name
Pass / Fail	Reduce WLAN Transmit power (TX) range to not work outside of office
Pass / Fail	WPA2 and AES Encryption Enabled
Pass / Fail	Do not use WEP

Pass / Fail	Disallow installing unnecessary software or applications
Pass / Fail	Perform an inventory of devices containing client data
Pass / Fail	Limit / Disable access to stored client data

Pass / Fail	RMM
Pass / Fail	Patch management on browsers?
Pass / Fail	Regular tune up scheduling?
Pass / Fail	Disable stored password feature

Pass / Fail	Printed and Readily Available?
Pass / Fail	Point of Contact Established
Pass / Fail	What happens if breached?

Pass / Fail	Is Calling IRS part of the plan? YES
Pass / Fail	Training Procedure YES
Pass / Fail	How to spot data theft? YES
Pass / Fail	Security and Awareness Training: [SecurityAwarenessTrainingMethod] YES

Cyber Security Policy

Information Types & Impact if Stolen:

	[redacted]	[redacted]	[redacted]	[redacted]
Cost of Revelation (Confidentiality)	Med	High	High	Low
Cost to Verify Information (Integrity)	High	High	High	Low
Cost of Lost Access	Med	High	High	Low
Cost of Lost Work	Low	High	High	Low
Fines, Penalties, etc	Med	High	High	Low
Legal Costs	Med	High	High	Low
Cost to Repair Problem	Low	High	High	Low
Overall Impact	**Med**	**High**	**High**	**Low**

Threats, Vulnerabilities, and the Likelihood of an Incident

	[redacted]	[redacted]	[redacted]	[redacted]
CONFIDENTIALITY				
Theft By Criminal	Low	Low	Low	Low
Accidental Disclosure	Low	Low	Low	Low

INTEGRITY				
Accidental Alteration by user / employee	Low	Low	Low	Low
Intentional Alteration by hacker / criminal	Low	Low	Low	Low
AVAILABILITY				
Accidental Destruction (fire, water, user error)	Low	Low	Low	Low
Intentional Destruction	Low	Low	Low	Low
Overall Likelihood	Low	Low	Low	Low

Inventory That Contains Client Information

1	backup drive			
2	home computer work			
3	laptop			
4	work computer office			
5				
6				
7				
8				
9				

Steps Taken to Protect Consumer Data / PII

Document Safety Measures

- Collect essential PII
- Use data encryption
- Limit staff access
- Software-dependent formats
- Discard files at 7 years
- Restrict PII access
- Enable 2FA
- Backup securely
- Regular audits
- Version control
- Shred physical copies
- Encrypt all drives

Use Security Software

- Antivirus: Installed Managed AV
- Antispyware: Managed AV
- Endpoint Detection & Response
- Intrusion Detection Systems
- Firewall
- Drive Encryption

Create Strong Passwords

- Minimum Password Length: 8
- Use capital / lower / number / symbol
- Do not reuse passwords
- Avoid personal information
- Use phrases instead of words
- Change default/temporary passwords
- Do not use your email as your username
- Store passwords in a password manager
- Do not tell your password to anyone
- Use MFA in all platforms

Secure Wireless Networks

- Change default admin password
- Minimize WLAN range
- Rename SSID to be vague
- Hide Public SSID
- Use WPA2-AES
- Avoid WEP
- Use VPN only
- Update firmware
- Enable MAC filtering
- Disable remote access
- Isolate guest network
- Monitor network activity

Protect Stored Client Data

- Use drive encryption
- Backup encrypted data
- Gapped cloud backup
- Avoid public USBs
- Skip extra software
- Inventory data devices
- Limit internet access
- Delete before disposal
- Destroy drives
- Multi-factor authentication
- Off-site secure storage
- Control user access
- Encrypt local storage
- Regular data audits
- Secure cloud storage
- Automated data wipes

Spot Data Theft

- Duplicate SSN filed
- Unexpected IRS letters
- Unfiled clients get refunds
- IRS account alerts
- EFIN count mismatch
- Phantom email replies
- Slow network speed
- User lockouts
- Software login errors
- Unusual file changes
- Mismatched forms
- Random pop-ups
- Unknown network devices
- Failed login attempts

Monitor EFIN / PTINs

- Weekly checks to make sure you flag any abuses
- https://rpr.irs.gov/datamart/mainMenuUSIRS.do
- Security Awareness Training:

Guard Against Phishing Scams

- Separate Personal & Business Email
- Secure Email with with 2FA
- Install anti phishing toolbar: [APName]
- Scan for malware
- Avoid opening unknown attachments
- Forward suspicious IRS emails
- Enable spam filter
- Use verified plugins
- Check URL before clicking
- Confirm sender identity
- Regular software updates
- Whitelist trusted source

Be Safe on the Internet

- Patch management on browsers & OS
  - ☑ 3rd Party Patch Management:
  - ☑ Windows Patch Management:
- Scan downloaded files before opening
- Tune Ups on a regular schedule
  - ☑ Method of Tune Ups:
- Avoid accessing business email from public Wi-Fi
- Look for "S" in HTTPS://
- Never Select Remember Passwords In A Browser

FTC Safeguards Rule

Employee Designated for Coordination: [FirstName] [LastName]

- [Proof of Their REAL WORLD Experience]

Annual reporting to the board of directors on any issues related to the information security program

Training and education programs will be utilized

Disposal Procedure – Will remove customer information that is no longer necessary for business operations or other legitimate business purposes with GAAP guidelines.

Safeguards have been designed to protect client data listed in plan.

A qualified provider with real world experience has been hired:

Service Providers

- Vet service providers
- Define security expectations
- Include monitoring clauses
- Schedule periodic reassessments
- Conduct background checks
- Require security certifications
- Audit provider compliance
- Require incident reporting

Current Risks to Customer Information

- Leaving the computer unattended: 2FA and Strong Password Protect
- Allowing unattended access to tech companies: Access restricted, 2FA
- Past people with access getting in: All passwords have been changed
- Brute Force Attacks: Long complex passwords and 2FA
- Stolen Computers: All hard drives are encrypted. Financial Information is on the Cloud.

Written Response Plan

- Define clear objectives for security incident response plan
- Establish procedures to activate during security events
- Outline roles, responsibilities, and decision-making hierarchy
- Facilitate internal and external communication channels
- Implement process to rectify identified system vulnerabilities
- Develop procedures for documenting and reporting incidents
- Conduct post-incident evaluations to analyze outcomes
- Regularly update incident response and security plans based on learnings

Employee Management and Training

Every new employee is required to sign a confidentiality agreement, adhering to the company's standards for safeguarding customer information. Access to this data is limited to those with a business need, like customer service reps, and only to the extent necessary for their tasks. To secure sensitive data, employees must use strong passwords, consisting of at least eight characters, a mix of upper and lower-case letters, numbers, and symbols, which must be changed regularly. Inactivity triggers a password-activated screensaver to lock workstations.

The company also has strict guidelines for the use and protection of mobile devices like laptops, PDAs, and cell phones. These must be securely stored when not in use and, if possible, should contain encrypted customer files to enhance security in case of theft. Staff are trained to follow these measures diligently to maintain the confidentiality and integrity of customer information.

- Locking rooms and file cabinets where records are kept
- Not sharing or openly posting employee passwords in work areas.
- Encrypting sensitive customer information
- Transferring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data
- Reporting suspicious attempts to obtain customer information to designated personnel.

Employees are regularly reminded of both the company's policy and the legal obligation to keep customer data confidential. This is reinforced through visible reminders in areas where sensitive information is stored. For remote workers, specific telecommuting policies are in place, addressing whether and how customer data can be accessed or stored at home.

Personal computers used for work must be equipped with proper security software. Any violation of security policies results in disciplinary action. Upon termination, employees lose access to customer information through immediate deactivation of their login credentials. Additionally, documents containing sensitive information are labeled as "Sensitive" or "For Official Business" to further enhance security, as recommended by the IRS.

Information Systems

- Secure data storage
- Enforce 2 Factor Authentication
- Locked storage areas
- Strong password access
- No Internet storage of files
- Secure backups
- Inventory equipment
- Use SSL/TLS
- Auto-secure transmission
- No email-sensitive data
- Encrypt sensitive emails
- Secure disposal of documents
- Retention manager assigned
- Vendor due diligence conducted
- Shred papers with confidential info
- Erase hardware data

Detecting and Managing System Failures

- Update security programs daily
- Install 3rd party software patches
- Regularly update Windows patches
- Maintain firewalls for internet protection
- Close unused ports in firewall
- Inform employees quickly of issues
- Monitor network logs for safety
- Use intrusion alerts for breach
- Watch data transfers to stop lost info
- Dummy account inside SaaS

In The Event of an Information Breach

Person In Charge: [FirstName] [LastName]

1. Contact the IRS to inform them of the breach via phone and Email
2. Contact Experts
3. Insurance Company
    a. Check to see if the policy covers breach mitigation expenses
4. Contacting Clients and Other Services
    a. FTC - idt-brt@ftc.gov
    b. Credit / ID theft protection agency- certain states require offering credit monitoring / ID theft protection to victims of ID theft.
        i. Equifax: (800) 997-2493
        ii. Experian: (888) 397-3742
        iii. TransUnion (800) 680-7289
5. Clients
    a. Contact closest FBI Field Office
    b. Determine disclosure process with law enforcement
    c. Send individual letters to all victims and inform them of breach
6. Have them fill out Form 14039 (Identity Theft Affidavit)
7. Contact tax software vendor
8. Legal Counsel

In The Event of Fire, Medical Emergency, Burglary, or Natural Disaster

In the Event of a Fire

- Shut down computers
- Disconnect from internet
- Bring them to a safe location

In the Event of a Medical Emergency

- Have a backup person designated with access

In the Event of a Burglary

- Call local police
- Call Backblaze to see if they can track device
- Wipe PII remotely from device

In the Event of a Natural Disaster

- Shut down computers
- Disconnect from internet
- Bring them to a safe location
- Utilize gapped backup procedures if there is physical damage to physical backup

Policies

Policy: Safeguarding Client PII for Employees & Contractors

Purpose:

To outline the necessary conduct and behaviors for the secure management of client personally identifiable information (PII) in digital and physical forms. All users of our information systems must read, sign, and adhere to these guidelines.

Email and Web Links:

- Exercise caution with unexpected email attachments or links.
- Verify the legitimacy of an email by contacting the sender directly.
- Hover over links to check the destination URL.
- Train staff to recognize and report phishing attempts.

Device Segregation:

- Maintain separate devices for personal and professional use.
- Avoid performing business-sensitive tasks on personal devices.
- Do not engage in non-work activities, like gaming or video streaming, on work devices.

Storage Media:

- Refrain from inserting personal or unknown storage devices into work computers or networks.
- Disable "AutoRun" for USB and optical drives to prevent unauthorized software installation.

Software Downloads:

- Download software only from reputable sources.
- Exercise caution with freeware and shareware.

Information Sharing:

- Be wary of social engineering attempts aiming to manipulate into revealing information.
- Report any solicitation for sensitive information to supervisors.
- Never disclose usernames, passwords, or technical specs of the system.

Pop-Up Ads:

- Ignore prompts from pop-up ads.
- Employ a pop-up blocker and only allow pop-ups from trusted sites.

Password Policy:

- Use complex passwords consisting of letters, numbers, and special characters, with a minimum length of 8 characters.
- Use multi-factor authentication for important systems.
- Change default and periodically update passwords.
- Online Business Practices:

- Utilize secure browser connections (HTTPS) for online business transactions.
- Regularly clear browser cache, temporary files, and history, especially after public computer use.

Adherence to these guidelines ensures compliance with best practices for safeguarding client PII, as recommended by NIST in Section 4 of NISTIR 7621, titled "Small Business Information Security: The Fundamentals".

Policy: PII Data Retention and Destruction Policy for Accountants (GAAP-Compliant)

The objective of this policy is to align with Generally Accepted Accounting Principles (GAAP) and govern the secure handling of personally identifiable information (PII) in paper and electronic formats. This policy outlines the retention period and secure destruction procedures for such records.

Data Retention:

- PII data must be retained for a period consistent with business needs and GAAP requirements.
- The maximum retention period for PII records is set at 7 years, as per GAAP guidelines.

Destruction of Paper-Based Records:

- Secure destruction methods for paper-based PII records upon reaching the end of their service life are:
- Cross-cut shredding
- Incineration

Destruction of Electronic Records:

- Secure destruction methods for electronic-based PII records at the end of their service life include:
- Overwriting the file directory
- Reformatting the storage drive
- Physically destroying drive disks to render them inoperable

Compliance with this policy ensures adherence to legal requirements and industry best practices.

Reviewed 12/1/24

Stephanie Denman