TECH4 Accountants

Information SECURITY PLAN

Date

PREPARED FOR:

COMPANY NAME

Mr. First, Last Name

Job Title Here

Company street address here, City State, Zip Codes

123-456-7890, 111-222-3333

email@OfficeTemplatesOnline.com

Performed by: <Company Name>

I.OBJECTIVE

The objective of <CompanyName> is to create and document the proper safeguards that are to be used in compliance with the GLBA, FTC Financial Privacy and Safeguards Rules. This will also serve as the documentation of all policies and procedures used inside <CompanyName> to protect its clients' Personally Identifiable Information (PII). PII in this context will be in regards to any identifiable information that can pick a specific individual.

PII Herein Includes:

A. Taxpayer information held inside tax prep software
B. Drivers License, Social Security number, Date of Birth
C. Current / Previous Employment History
D. Previous tax returns, financial information like statements, and credit card numbers
E. E-mail addresses

PII shall not include information that is obtained from publicly available sources such as a Mailing Address or Phone Directory listing; or from federal, state or local government records lawfully made available to the general public.

II. PURPOSE

A. Document and show auditors / clients / prospects the data safeguards and policies.
B. Demonstrate how we can reasonably protect PII from outside influences.
C. Protect clients' from unauthorized access that can result in identity theft or fraud.

III. SCOPE

The Scope of the WISP shall be limited to the following protocols:

A. Recognize locations of PII and address vulnerabilities & measures taken to prevent breach..
B. Determine damage and consequences of breach to the company and its clients.
C. List current measures taken to prevent the breach from happening.

Regular monitoring and assessment of the effectiveness of aforementioned safeguards.

Taxes-Security-Together: Security Six Checklist

Activate anti-virus software.	Pass	Fail	Notes
	☐	☐	Antivirus Installed: <Vendor Name>
	☐	☐	Anti Spyware Installed < Vendor Name>
	☐	☐	Antiphishing Toolbar < Vendor Name>
Use a firewall.			
	☐	☐	Firewall < Vendor Name>
Two-Factor Authentication			
	☐	☐	Windows / Login
	☐	☐	Accessing Customer Data
Use backup software/services.			
	☐	☐	Cloud / On Prem / Both?
	☐	☐	Is it encrypted?
Use Drive encryption.			
	☐	☐	Encryption Through: <Method>
Create and secure Virtual Private Networks.			
	☐	☐	VPN < Vendor Name>
	☐	☐	
IRS Publication 4557: Safeguarding Taxpayer Data			
Create Strong Passwords			
	☐	☐	Enforce Password History: 24 (max) passwords remembered
	☐	☐	Minimum of 8 characters
	☐	☐	Password must meet complexity requirements: Enabled
	☐	☐	Avoid personal information use phrases instead
	☐	☐	Change default/temporary passwords that come with accounts including printers
	☐	☐	Store passwords in a secure location like a safe or locked file cabinet
	☐	☐	Use a password manager program but protect it with a strong password
	☐	☐	Use MFA for returning users
	☐	☐	Hasn't been involved in any major breaches

Notes From Tech4Accountants (Rush Tech Support):

While this plan is meant to be used for compliance with IRS & FTC Guidelines, we cannot guarantee compliance without having a technician confirm the statements in the plan. If you would like an expert to do the WISP for you, you can Save $500 by using the link www.tech4accountants.net/buy-wisp

TECH4 Accountants

Secure Wireless Networks (Pass / Fail)			
	☐	☐	Default login on router?
	☐	☐	Turn off public SSID
	☐	☐	Change guest wireless network to unidentifiable name
	☐	☐	Reduce WLAN Transmit power (TX) range to not work outside of office
	☐	☐	WPA2 and AES Encryption Enabled
	☐	☐	Do not use WEP
	☐	☐	Don't use anything other than your VPN to check email
Protect Stored Client Data (Pass / Fail)			
	☐	☐	Disallow installing unnecessary software or applications
	☐	☐	Perform an inventory of devices containing client data
	☐	☐	Limit / Disable access to stored client data
Safety (Pass / Fail)			
	☐	☐	Patch management on browsers?
	☐	☐	Regular tune up scheduling?
	☐	☐	Disable stored password feature in OS
Create a Data Security Plan (Pass / Fail)			
	☐	☐	Printed and Readily Available?
	☐	☐	Point of Contact Established
	☐	☐	What to happen if breached?
	☐	☐	Is Calling IRS part of the plan?
	☐	☐	Training Procedure
	☐	☐	How to spot data theft?
	☐	☐	Security and Awareness Training

Notes From Tech4Accountants (Rush Tech Support):

While this plan is meant to be used for compliance with IRS & FTC Guidelines, we cannot guarantee compliance without having a technician confirm the statements in the plan. If you would like an expert to do the WISP for you, you can Save $500 by using the link www.tech4accountants.net/buy-wisp

TECH4 Accountants

Cyber Security Policy

Information Types & Impact if Stolen:

	Customer Contact Information	Customer Tax Returns	Customer Billing Information	Personal Information
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

	Customer Contact Information	Customer Tax Returns	Customer Billing Information	Personal Information
CONFIDENTIALITY				
Theft By Criminal	Low (Encrypted, PW Protected, 2FA, VPN)	Low (Encrypted, PW Protected, 2FA, VPN)	Low (Encrypted, PW Protected, 2FA, VPN)	Low (Encrypted, PW Protected, 2FA, VPN)
Accidental Disclosure	Low	Low	Low	Low
INTEGRITY				
Accidental Alteration by user / employee	Low (1 person has access)	Low (1 person has access)	Low (1 person has access)	Low (1 person has access)
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: (Intentional Blanks for Growth)

	Description	Location	Type of Info	Potential Impact
1	<Example>	Cloud (8.8.8.8)	All client returns, billing information, tax information, contact information, social security	High
2	<Example>	Mobile	Personal, email, RDP to AWS	Med
3	<Example>	Mobile	Personal, email, RDP to AWS	Med
4	<Example>	Mobile	Personal, Email, Photos	Low
5	<Example>	Mobile	Personal, email, RDP to AWS	Med
6				
7				
8				
9				
10				

Steps Taken to Protect Consumer Data / PII

Document Safety Measures

- During the intake process, only PII that is required will be gathered.
- All data will be transmitted and contained via encrypted methods.
- PII will be accessible from employees on an as-needed basis.
- Formats will be subject to the software used in the collection process.
- Documents will be destroyed at the seven year mark.
- Only tax software and authorized parties will have access to PII.

Use Security Software

- Antivirus: Installed Managed AV (Company)
- Antispyware: Managed AV (Company)
- Firewall: (Company)
- Drive Encryption: (Company)

Create Strong Passwords

- Minimum of 8 characters
  - Minimum Password Length: 8
- Combination of letters, numbers, and symbols
  - Password must meet complexity requirements: Enabled
- Do not reuse passwords
  - Enforce Password History: 24 (max) passwords remembered
- Avoid personal information use phrases instead
- Change default/temporary passwords that come with accounts including printers
- Do not use your email as your username (when possible)
- Store passwords in a secure location like a safe or locked file cabinet
- Do not tell your password to anyone for any reason
- Use a password manager program but protect it with a strong password
- Use MFA for returning users

Secure Wireless Networks

- Change default admin on router. Use strong unique password
- Reduce wireless range in WLAN settings to lower Transmit power (TX) to the lowest where it still works in the office.
- Change the name of your router (SSID) to something that is not identifying
- Turn off SSID so it cannot be seen by those who do not need it
- Use WPA2 with AES for encryption
- Do not use WEP to connect devices
- Do not use a public Wi-Fi - only use VPN

Protect Stored Client Data

- Use drive encryption
  - (Company)
- Backup encrypted copies

- Avoid attaching USB drives with client data to public computers
- Avoid installing unnecessary software or applications
- Perform an inventory of devices where client data are stored (laptops, smart phones, tablets, external hard drives, etc.)
- Limit or disable internet access capabilities for devices that have stored taxpayer data.
- Delete all electronic information from devices, hard drives, USBs, etc. before throwing them away
- Physically destroy all drives that hold client data by shredding or burning before throwing away.

Spot Data Theft

- Client e-file is rejected because returned with their social security have already been filed
- Clients who haven't filed begin receiving authorization letters 5071C, 4883C, 5747C, from the IRS
- Clients who haven't filed taxes receive refunds
- Clients who use the IRS website get notifications that their account was accessed, disabled, or created
- The number of returns filed with tax practitioner's EFIN exceeds number of clients
- Tax professional / client replying to emails that were never actually sent.
- Network computers are running slower than usual
- Computer cursor moving or changing numbers without touching the keyboard
- Network computers locking out tax practitioners.

Monitor EFIN / PTINs

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

Recognize Phishing Scams

- Security Awareness Training: (Company)

Guard Against Phishing Scams

- Separate personal and business email accounts with 2FA
- Install anti phishing toolbar: (Company)
- Use security to scan for malware and scan emails for viruses
- Never open or download attachments from unknown senders
- Send only password-protected and encrypted documents if you must share files via email
- Do not respond to suspicious emails, forward to phishing@irs.gov if they are IRS related

Be Safe on the Internet

- Patch management on browsers
  - 3rd Party Patch Management (Company)
  - Windows Patch Management: (Company)
- Scan downloaded files before opening
- Tune Ups on a regular schedule
  - (Company)

- Look for "S" in HTTPS://
- Avoid accessing business email from public Wi-Fi
- Disable stored password feature in OS

FTC Safeguards Rule

Employee Designated for Coordination: <OWNER> (Owner) & (Name/Company) (CISO)
Annual reporting to the board of directors on any issues related to the information security program
Training and education programs will be utilized

Audit trails done through (Company) to see who is doing what and when
Disposal Procedure – Will remove customer information that is no longer necessary for business operations or other legitimate business purposes

Current Risks to Customer Information:

- Leaving the computer unattended: 2FA and Strong Password Protects
- 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 Cloud.
- (IT Company and How They Protect Your Data)

Employee Management and Training

Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.

Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.

Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.) (IRS suggestion: passwords should be a minimum of eight characters.)

Use password-activated screen savers to lock employee computers after a period of inactivity.

Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device. Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:

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

Regularly remind all employees of your company's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.

Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.

Impose disciplinary measures for security policy violations. Prevent terminated employees from accessing customer information by immediately deactivating their passwords and usernames and taking other appropriate measures. (IRS Suggestion: Add labels to documents to signify importance, such as "Sensitive" or "For Official Business" to further secure paper documents.)

Information Systems

Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:

- Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.
- Store records in a room or cabinet that is locked when unattended.
- When customer information is stored on a server or other computer, ensure that the computer is accessible only with a "strong" password and is kept in a physically secure area.
- Where possible, avoid storing sensitive customer data on a computer with an Internet connection.
- Maintain secure backup records and keep archived data secure by storing it offline and in a physically secure area.
- Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored steps to ensure the secure transmission of customer information.
- When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit. (IRS Suggestion: Transport Layer Security 1.1 or 1.2 is newer and more secure.)
- If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.
- If you must transmit sensitive data by email over the Internet, be sure to encrypt the data.
- Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule

- Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
- Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.
- Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.

Detecting and Managing System Failures

Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:

- Check with software vendors regularly to get and install patches that resolve software vulnerabilities.
- Use anti-virus and anti-spyware software that updates automatically;
- Maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations
- Regularly ensure that ports not used for your business are closed;
- Promptly pass along information and instructions to employees regarding any new security risks or possible breaches. Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to:
- Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information;
- Use an up-to-date intrusion detection system to alert you of attacks;
- Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and
- Insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges. Take steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach.

In The Event of Information Breach:

Person In Charge: <OWNER>

1. Contact the IRS to inform them of breech via phone and Email
    a. (FIND YOUR AREA) Area 4 (FL, GA, NC, NY, SC, TX)
        i. (216) 415-3518 / (401) 528-1819
        ii. CL.SL.Area.4@irs.gov
2. Contact Local Governing FBI Field Office to report breech:
    a. (FIND YOUR AREA) (754) 703-2000
        i. Contact Local Secret Service (only if instructed)
3. Contact Local Police to Report on the data breach
    a. (FIND YOUR AREA) Lake Worth Police Department:
        i. (561) 688-3000
4. Contact States in Which You Prepare State Returns

a. Email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states.
b. State Attorneys General for each state in which you prepare returns.

5. Contact Experts:
    a. Tech4Accountants
        i. (877)572-6989 to identify cause of breach and how to remediate
    b. Insurance Company
        i. Check to see if policy covers breach mitigation expenses
6. Contacting Clients and Other Services
    a. FTC
        i. 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. Trans Union (800) 680-7289
c. Clients
        i. (Speak with Law Enforcement First to Establish When) Send individual letter to all victims and inform them of breach
            1. (FIND YOUR AREA REQS) Florida requires mail or email notification within 30 days
        ii. Have them fill out Form 14039 (Identity Theft Affidavit)

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

1. Roles & Responsibilities
    - <OWNER> controls situation and will perform necessary steps
2. What to do with information?
    - Shut down computers
    - Disconnect from internet
3. Who to call in case of an incident?
    - Tech4Accountants / Rush Tech Support (877)572-6989

List Out Required Software:

- Antivirus:
- Anti-Spyware:
- Firewall:
- Password Manager:
- 2FA:
- Backup:
- Windows Patch Management:
- 3rd Party Patch Management:
- Security Awareness Training:

Final Instructions

Get plan audited & approved by a licensed cyber security expert in the accounting and WISP field
Print and get a professional copy at a print shop with a spiral bound
Keep in office and update annually

If you need assistance visit https://tech4accountants.net/irs-wisp-review/ or call (877) 572-6989.

Signature: _____ Date: _____
PTIN Holder or Firm Owner

Signature: _____ Date: _____
Signature of Data Security Coordinator

Contact US

Call: +877-572-69890

Email: support@tech4accountants.net

TECH4 Accountants

Thank You

www.tech4accountants.net