Communications & Liaison
STAKEHOLDER LIAISON

Developing A Written Information Security Plan

Media: CL.SL.Web.Conference.Team@IRS.gov

Communications & Liaison
STAKEHOLDER LIAISON

Technology Problems?

- Audio is available through your computer only.

  There is no call-in number.
- Make sure your computer sound is not muted.
- See Technical Help document posted to "Materials" on viewing screen for tips and required settings.
- Still Problems?
  - Close & re-launch your player…OR…
  - Click on settings on your browser viewing screen.
  - Select "HLS."

Communications & Liaison
STAKEHOLDER LIAISON

Developing A Written Information Security Plan

Presented by
Security Summit

November 30, 2023

Developing A Written Information Security Plan
2023 IRS Tax Forum

Jared Ballew

2022-23 ETAAC - Chairman

IRS Security Summit - Tax Pro Workgroup Co-Lead

Vice President of Government Relations
Drake Software & TaxAct

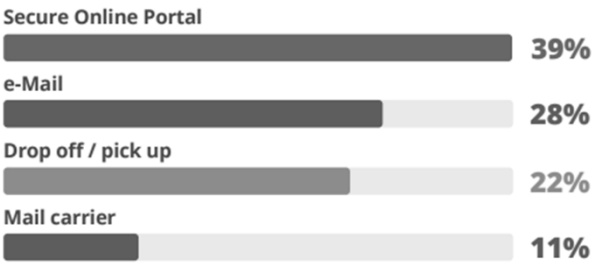
Rev. 11/21/23

Agenda

- Explain the FTC Safeguards Rule
- Explain a tax professional's obligation to protect taxpayer data
- Identify the basic steps to data security
- Outline how to create a Written Information Security Plan (WISP)
- Describe signs of data theft
- List the steps to take if you are a victim of a data breach

Tax Office – Changing Landscapes

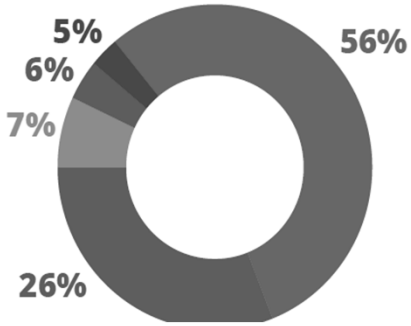
How were you most likely to exchange important tax documents with those clients who didn't come into the office?



Tax Office – Changing Landscapes

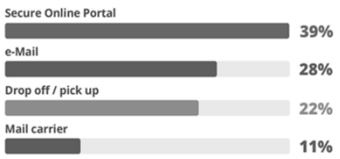
What is the main way you communicated with clients who didn't come into the office?

- e-Mail
- Phone
- Text
- Virtual meeting software
- Portal messaging



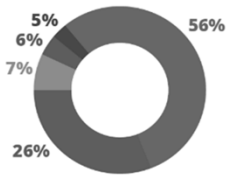
Tax Office – Changing Landscapes

How were you most likely to exchange important tax documents with those clients who didn't come into the office?



What is the main way you communicated with clients who didn't come into the office?

- e-Mail
- Phone
- Text
- Virtual meeting software
- Portal messaging



Considerations:

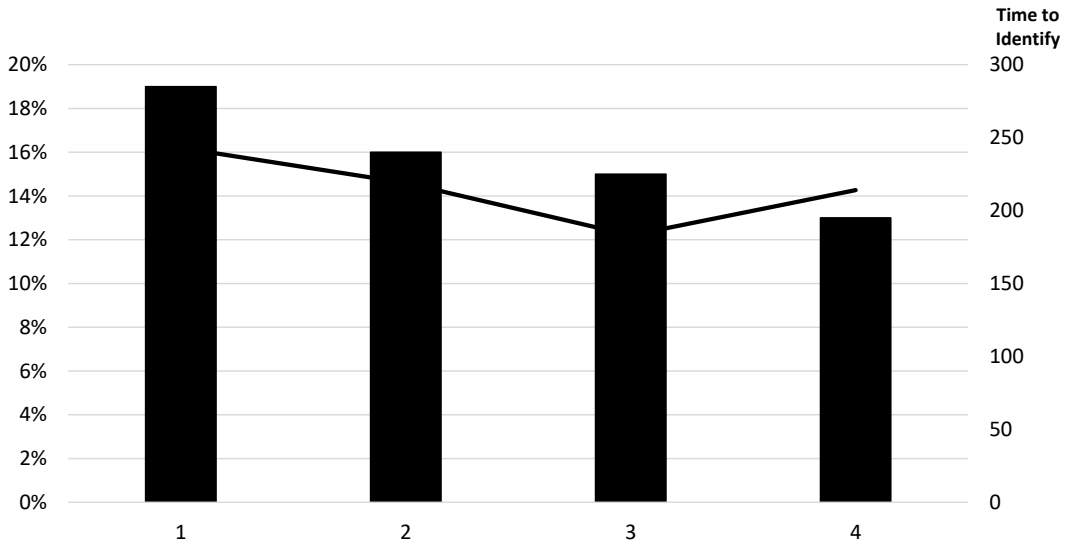
- Tax data is money for fraudsters
- Refundable credits
- Ransomware
- Re-directed refunds
- Remote tax prep – "Know your Customer"
- Protect yourself AND your practice
- Beyond tax data

Data Breach Statistics

- In 2022 $8.8 billion lost to scams
- Investment and Impersonator scams
- YOUNGER (20-29) reported losing more often than OLDER (70-79) but older lost more per incident
- Average time to identify data breach - 277 Days (60-80 days to contain) Ransomware +49 days
- What is “Zero Trust”? (Everyone authenticates)
- 1 in 3 home computers are infected with malicious software
- 600k accounts are hacked every single day
- 31% of millennials share their passwords

Source: IBM Cost of Data Breach 2022 / CISA.gov / https://consumer.ftc.gov/consumer-alerts/2023/02/top-scams-2022

Data Breach Statistics



Source: IBM Cost of Data Breach 2022

What is Security?

FTC SAFEGUARDS RULE

- Physical
- Technical
- Administrative

Source: https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,the%20development%20of%20security%20systems.

Physical Safeguards

Keep Your Data Safe From Physical Threats

Examples of **physical safeguards** include limiting access to computers that store client data or creating a backup and storing it in a secure location offsite

Technical Safeguards

Ensure That Your Network Is Not Compromised

Technical safeguards include updated anti-malware and antivirus software on office devices

Administrative Safeguards

Manage and Train Your Staff

Employees are the leading cause of data breaches. Ensure that they can recognize phishing emails and other attempts by malicious actors to compromise data.

Polling Question #1

Which statement below is part of the FTC Safeguards rule:

a. **Limit access to computers that store client data**
b. **Update anti-malware and antivirus software on office devices**
c. **Ensure that employees can recognize phishing emails**
d. **All of the above**

Cyber Hygiene

Question Everything - Trust Nothing

Cyber Hygiene Best Practices

Separate **personal & business** accounts when possible

- Email Addresses
- Wi-Fi Networks
- Employee Devices
- Web Searched or Surfing

Cyber Hygiene Best Practices

Be aware of application and device **Privacy Settings**

- Location Sharing
- Microphones and Camera Settings
- Automated Backup Tools
- Social Media
- Internet of Things (IoT)

Cyber Hygiene Best Practices

Attacks happen **beyond just email**

- **Vishing:** Often the caller will pretend to be calling from the government or tax authority
- **Smishing:** Text messages with malicious links to webpages, email addresses, or phone numbers that when clicked may automatically open a browser window or email message or dial a number
- **QRishing:** Form of phishing initiated using malicious QR codes embedded in emails, texts, posters, magazines, brochures, or menu-less restaurants

Polling Question #2

True or False: A best practice to maintain "Cyber Hygiene" is to question everything and trust nothing.

a. True

b. False

Your Obligation

Protecting Taxpayer Data is the Law

- Gramm-Leach-Bliley Act (GLBA)
- IRS Pub 4557
- FTC Data Breach Response Guide

Gramm-Leach-Bliley Act

A U.S. law that requires financial institutions to **protect consumer data**

- Tax and accounting professionals are considered financial institutions, *regardless of size*
- The Federal Trade Commission (FTC) is responsible for the GLBA's implementation
- FTC issued the Safeguards Rule to outline data safety measures

IRS Publication 4557

Safeguarding Taxpayer Data

Polling Question #3

Which statement is true regarding The Gramm-Leach-Bliley Act:

a. Tax and accounting professionals are not considered financial institutions

b. Tax and accounting professionals are considered financial institutions, *regardless of size*

c. The IRS is responsible for the Gramm-Leach-Bliley Act implementation

d. Both A and C are true

IRS Pub 4557

A guide for the **FTC Safeguards Rule**

- The Safeguards Rule dictates that tax return preparers must create and enact Written Information Security Plans (WISPs) to protect client data
- The Safeguards Rule requirements are flexible so that companies can implement safeguards appropriate to their own circumstances

Basic Steps

- Install Software Updates
- Use anti-virus/anti-malware
- Secure Email –
  - Turn on 2FA / MFA
  - Secure against SSN etc.. (Google tools for example)
- Create Strong Password (Password Managers)
- Encrypt Files
- Secure Wireless Networks
- Create your WISP
- Change Factory Passwords
- Backup Everything

Review

The FTC Requires each firm to:

- Designate one employee to coordinate the information security program
- Identify and assess the risks to customer information
- Design and implement a safeguards program (WISP)
- Select service providers that can maintain appropriate safeguards
- Evaluate and adjust your security program considering relevant circumstances
- Multi-Factor Authentication (NEW)

Polling Question #4

True or False: The Federal Trade Commissions (FTC) requires a Written Information Security Plan (WISP).

a. **True**

b. **False**

IRS Publication 5708

Creating a Written Information Security Plan for your Tax & Accounting Practice

Your Security Plan

Ensure that your security policies are appropriate to your company's:

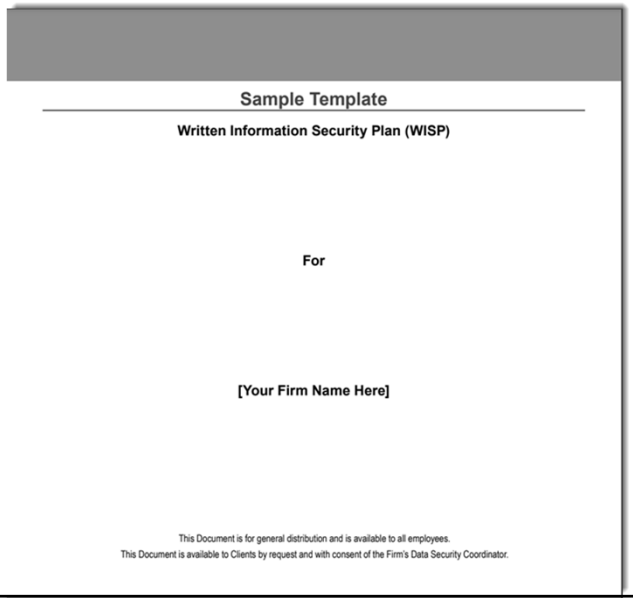
- Size
- Complexity
- Scope of activities
- Sensitivity of customer data

Creating your WISP

There is no one-size-fits-all Security Plan

Any good WISP should focus on 3 areas:

- Employee management and training
- Information systems
- Detecting and managing system failures



Sample Template

Written Information Security Plan (WISP)

For

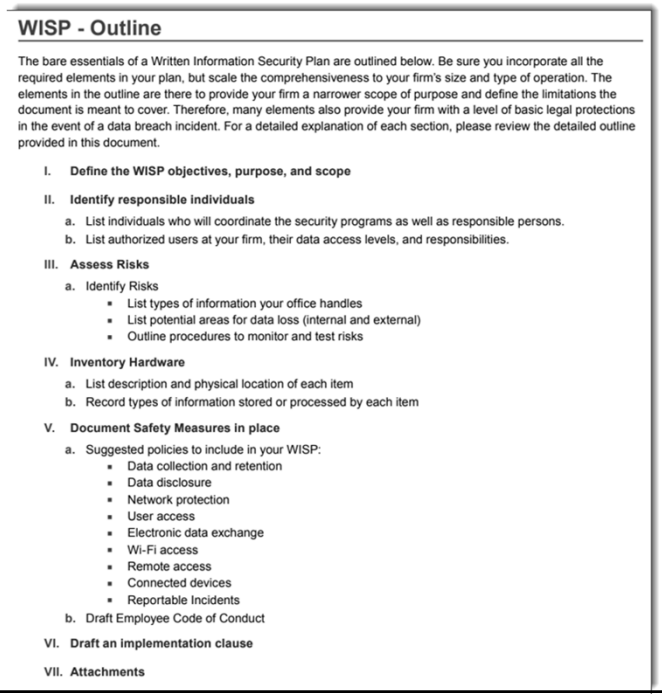
[Your Firm Name Here]

This Document is for general distribution and is available to all employees.
This Document is available to Clients by request and with consent of the Firm's Data Security Coordinator.

WISP Outline

A starting point for developing your plan

- Begin with your plan's objectives, purpose, and scope
- Identify responsible individual
- Assess Risks
- Inventory Hardware
- Document Safety Measures
- Draft an implementation clause
- Ancillary attachments



WISP - Outline

The bare essentials of a Written Information Security Plan are outlined below. Be sure you incorporate all the required elements in your plan, but scale the comprehensiveness to your firm's size and type of operation. The elements in the outline are there to provide your firm a narrower scope of purpose and define the limitations the document is meant to cover. Therefore, many elements also provide your firm with a level of basic legal protections in the event of a data breach incident. For a detailed explanation of each section, please review the detailed outline provided in this document.

I. **Define the WISP objectives, purpose, and scope**

II. **Identify responsible individuals**
   a. List individuals who will coordinate the security programs as well as responsible persons.
   b. List authorized users at your firm, their data access levels, and responsibilities.

III. **Assess Risks**
   a. Identify Risks
      - List types of information your office handles
      - List potential areas for data loss (internal and external)
      - Outline procedures to monitor and test risks

IV. **Inventory Hardware**
   a. List description and physical location of each item
   b. Record types of information stored or processed by each item

V. **Document Safety Measures in place**
   a. Suggested policies to include in your WISP:
      - Data collection and retention
      - Data disclosure
      - Network protection
      - User access
      - Electronic data exchange
      - Wi-Fi access
      - Remote access
      - Connected devices
      - Reportable Incidents
   b. Draft Employee Code of Conduct

VI. **Draft an implementation clause**

VII. **Attachments**

Polling Question #5

Which one of the following is NOT a focus area of a Written Information Security Plan (WISP)?

a. Information systems

b. Advertising campaigns and publicity

c. Detecting and managing system failures

d. Employee management and training

Drafting Security Policies

Security Plans Tailored to your Business

Common Security Policies

Policies to consider include, but are not limited to:

- Physical Access Policy
- Contingency Policy
- Security Software Policy
- Password Policy
- Network Policy
- Confidential Data Policy
- Breach Notification Policy
- Remote Work Policy

Be On Guard

- Spot data theft
- Monitor EFIN
- Phishing scams
- Internet usage

Signs of Data Theft

- The number of returns filed with the tax professional's Electronic Filing Identification Number (EFIN) exceeds the number of clients
- Tax professionals or clients responding to emails that the firm did not send
- Network computers running slower than normal
- Computer cursors moving or changing numbers without touching the keyboard
- Network computers locking out employees

Signs of Data Theft

- Clients' e-filed returns reject because of duplicate SSN
- A taxpayer checks Where's My Refund and it shows as processed but they haven't filed yet.
- Clients who haven’t filed tax returns begin to receive taxpayer authentication letters (5071C, 4883C, 5747C) from the IRS
- Clients receive unrequested refunds or tax transcripts
- Clients who created an IRS online services account receive an IRS notice that their account was accessed or IRS emails stating their account has been disabled. Or clients unexpectedly receive an IRS notice that an IRS online account was created in their names

What if the worst happens?

Activate Your Plan (WISP)

- Contact IRS and States
- Contact law enforcement (Local/FBI)
- Contact insurance carrier
- Contact experts (Software and Service providers)
- FTC : Data Breach Response: A Guide for Businesses

Polling Question #6

What should a tax professionals do if she/he is a victim of a data breach?

a. **Contact insurance carrier, law enforcement and experts**
b. **Contact IRS Stakeholder Liaison and States**
c. **None of the above**
d. **Both A and B**

FTC Data Breach Response Guide

Document that guides practitioners through the **steps to take** in the event of a breach

- Secure operations, fix vulnerabilities, notify appropriate parties, and inform clients
- Implementing and monitoring a Written Information Security Plan is an effective tool against breaches
- Failures that lead to an unauthorized disclosure may subject you to penalties under Sections 7216 and/or 6713 of the Internal Revenue Code (IRS Pub 1345, pg. 8)

Key Points

- Separate your work and personal devices, network, and email accounts.
- Train your staff on how to use cyber hygiene in order to protect taxpayer data from internal and external threats.
- Prioritize protecting your email. Think before you click or open.
  - Scan every document you receive with anti-virus software before opening it.

Communications & Liaison
STAKEHOLDER LIAISON

Upcoming Webinars

- **For information on future webinars, visit IRS.gov and use keyword search "webinars".**
- **Visit the IRS Video Portal for a variety of video and audio topics.**
- **www.irsvideos.gov**

THANK YOU!