Practical Guide to Writing YOUR Data Security Plan

American Society of Tax Problem Solvers

Bill Nemeth, EA
WGNemeth@aol.com

ASTPS

Bill Nemeth, EA

WGNemeth@aol.com

15 years as an Enrolled Agent
30+ Years as a tax Professional
Currently GAEA President & GAEA Education Chair

Bachelors degree in Automotive Engineering
(Kettering Institute (formerly GMI))
Masters degrees (MIT) in Mechanical Engineering
MBA in Marketing (Wayne State University)

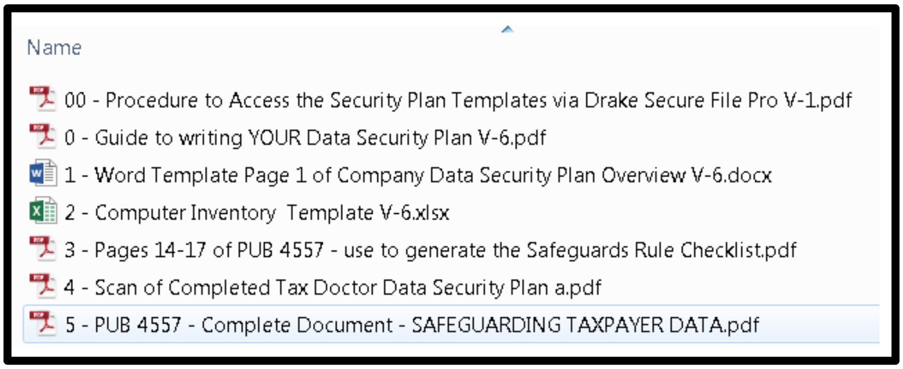
Prepares & presents live programs and webinar programs on timely federal tax topics.

In his spare time, he and his wife Merry Brodie are amateur beekeepers.

ASTPS

Download Files

PDF of Slides – 2 Slides per Page



Name

- 00 - Procedure to Access the Security Plan Templates via Drake Secure File Pro V-1.pdf
- 0 - Guide to writing YOUR Data Security Plan V-6.pdf
- 1 - Word Template Page 1 of Company Data Security Plan Overview V-6.docx
- 2 - Computer Inventory Template V-6.xlsx
- 3 - Pages 14-17 of PUB 4557 - use to generate the Safeguards Rule Checklist.pdf
- 4 - Scan of Completed Tax Doctor Data Security Plan a.pdf
- 5 - PUB 4557 - Complete Document - SAFEGUARDING TAXPAYER DATA.pdf

This is File 0

Guide to Creating YOUR Data Security Plan

File 0 - Instructions on how to download and use these files to create your Data Security Plan.

File 1 - Word Template - Page 1 of your Data Security Plan Edit to include your information – then print.

File 2 - EXCEL Computer Inventory Template - Page 2 of your Data Security Plan - Edit to include your information – then print.

File 3 - Print out these pages (14 - 17 of IRS Pub 4557 Safeguarding Taxpayer Data) which you will then complete by checking the applicable box for each data security item. This becomes page 3-6 of your Data Security Plan.

File 4 – **Example** of a COMPLETED Data Security Plan. This is how your plan will look when finished.

File 5 – A complete copy of IRS Pub 4557 – For Reference only.

Practical Guide to Writing YOUR Data Security Plan

You must HAVE a Data Security Plan per the FTC (Federal Trade Commission).

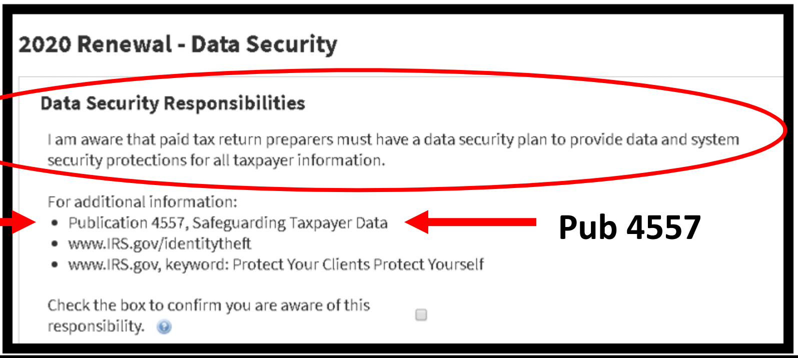
See the warning when you renew your PTIN on the following page.

5

2020 PTIN Renewal

Added statement on 2020 PTIN Renewal

Screen Shot Shown Below



2020 Renewal - Data Security

Data Security Responsibilities

I am aware that paid tax return preparers must have a data security plan to provide data and system security protections for all taxpayer information.

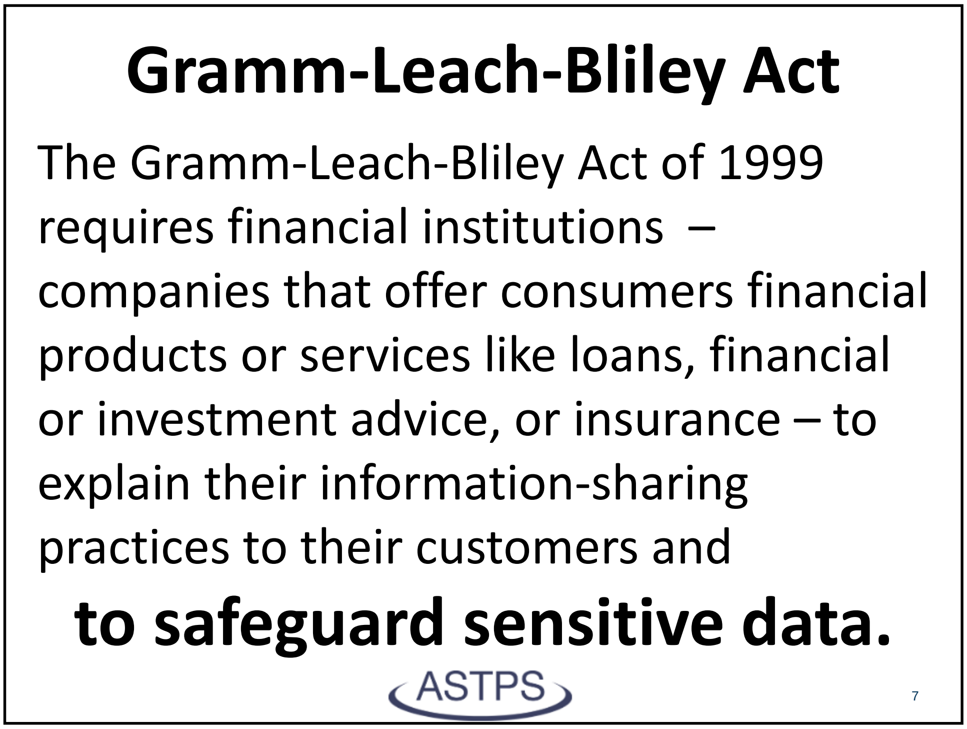
For additional information:

- Publication 4557, Safeguarding Taxpayer Data
- www.IRS.gov/identitytheft
- www.IRS.gov, keyword: Protect Your Clients Protect Yourself

Check the box to confirm you are aware of this responsibility. □

Pub 4557

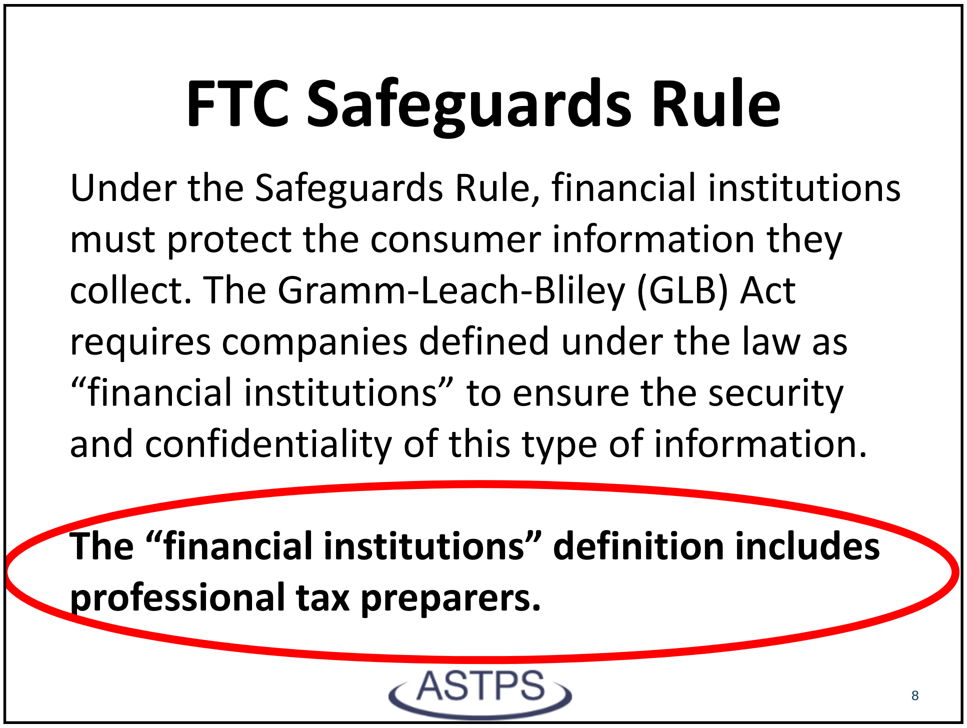
6



Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act of 1999 requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and

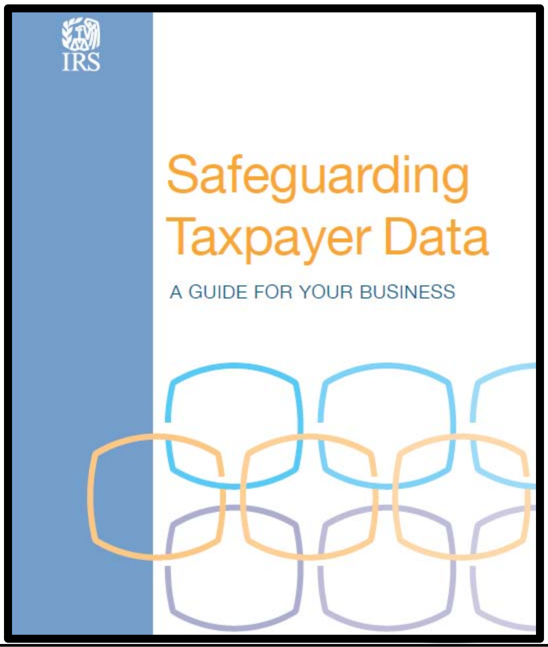
to safeguard sensitive data.



FTC Safeguards Rule

Under the Safeguards Rule, financial institutions must protect the consumer information they collect. The Gramm-Leach-Bliley (GLB) Act requires companies defined under the law as “financial institutions” to ensure the security and confidentiality of this type of information.

The “financial institutions” definition includes professional tax preparers.



IRS

Safeguarding Taxpayer Data

A GUIDE FOR YOUR BUSINESS

Data Security Plan will be based on IRS Pub 4557

Included as 5 - PUB 4557

Review of IRS Pub 4557 Guide to your business

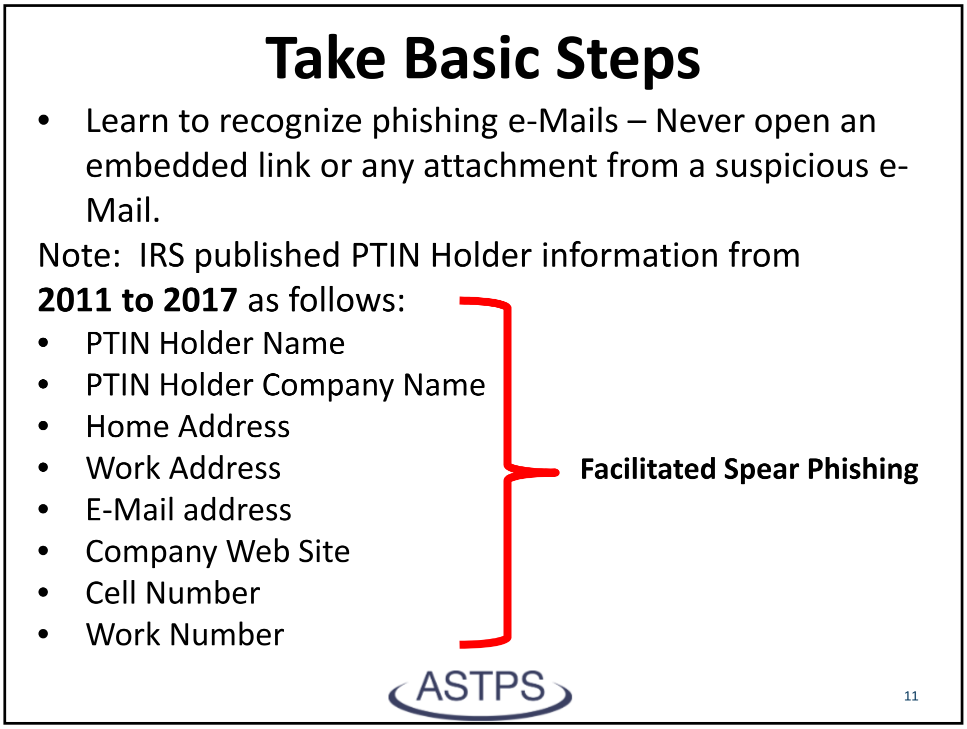
Understand basic security steps and how to take them

Recognize the signs of data theft and how to report data theft

Respond and recover from a data loss

Understand & comply with the FTC Safeguards Rule.

ASTPS



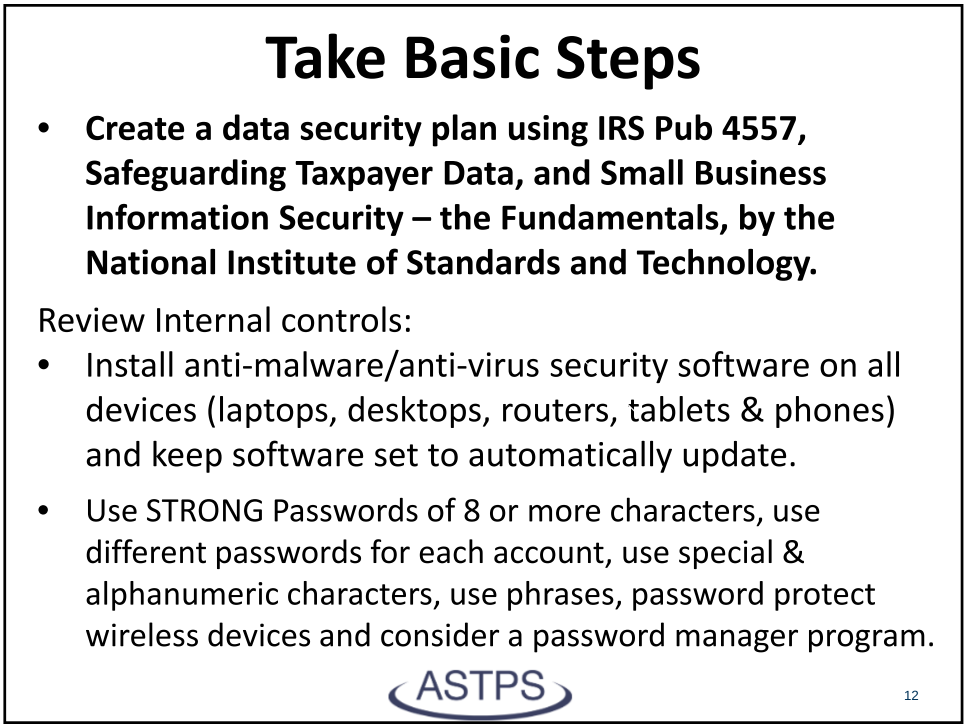
Take Basic Steps

- Learn to recognize phishing e-Mails – Never open an embedded link or any attachment from a suspicious e-Mail.

Note: IRS published PTIN Holder information from **2011 to 2017** as follows:

- PTIN Holder Name
- PTIN Holder Company Name
- Home Address
- Work Address
- E-Mail address
- Company Web Site
- Cell Number
- Work Number

Facilitated Spear Phishing

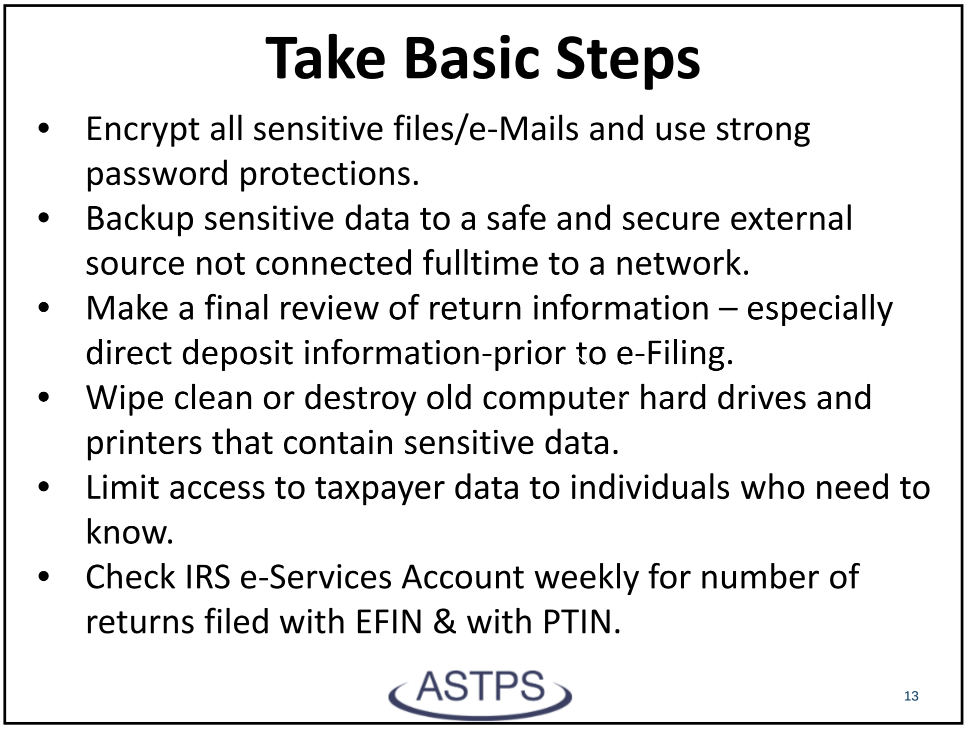


Take Basic Steps

- **Create a data security plan using IRS Pub 4557, Safeguarding Taxpayer Data, and Small Business Information Security – the Fundamentals, by the National Institute of Standards and Technology.**

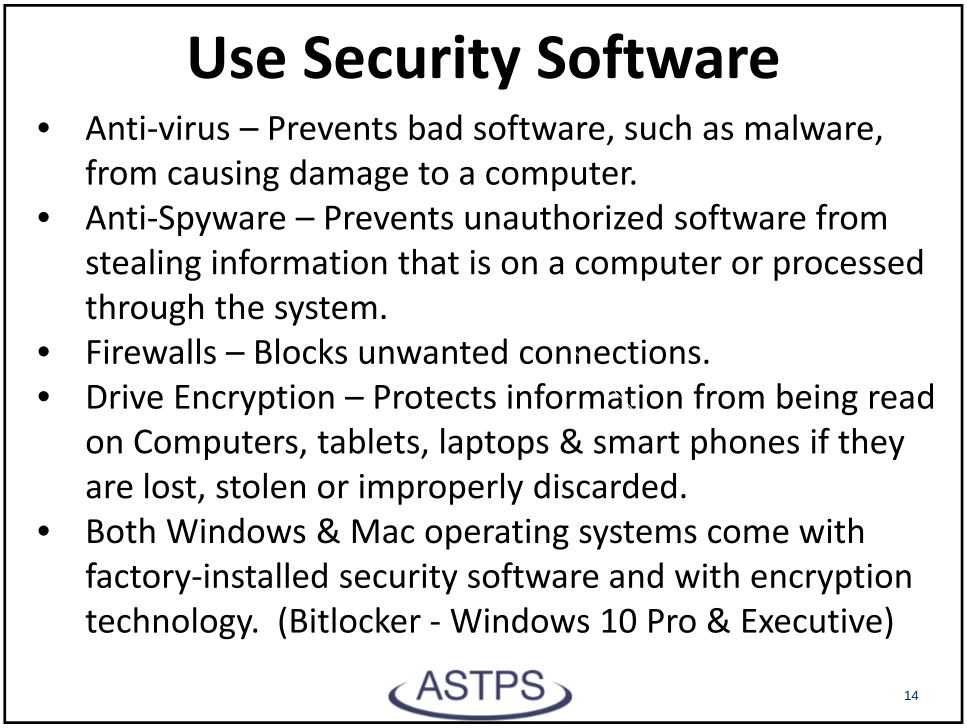
Review Internal controls:

- Install anti-malware/anti-virus security software on all devices (laptops, desktops, routers, tablets & phones) and keep software set to automatically update.
- Use STRONG Passwords of 8 or more characters, use different passwords for each account, use special & alphanumeric characters, use phrases, password protect wireless devices and consider a password manager program.



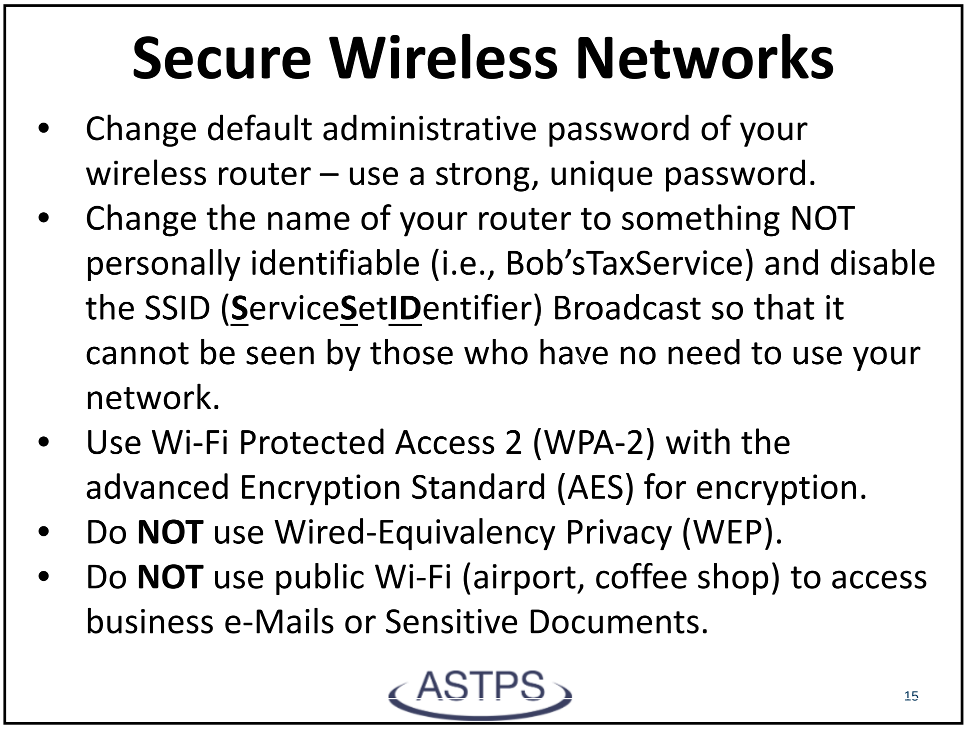
Take Basic Steps

- Encrypt all sensitive files/e-Mails and use strong password protections.
- Backup sensitive data to a safe and secure external source not connected fulltime to a network.
- Make a final review of return information – especially direct deposit information-prior to e-Filing.
- Wipe clean or destroy old computer hard drives and printers that contain sensitive data.
- Limit access to taxpayer data to individuals who need to know.
- Check IRS e-Services Account weekly for number of returns filed with EFIN & with PTIN.



Use Security Software

- Anti-virus – Prevents bad software, such as malware, from causing damage to a computer.
- Anti-Spyware – Prevents unauthorized software from stealing information that is on a computer or processed through the system.
- Firewalls – Blocks unwanted connections.
- Drive Encryption – Protects information from being read on Computers, tablets, laptops & smart phones if they are lost, stolen or improperly discarded.
- Both Windows & Mac operating systems come with factory-installed security software and with encryption technology. (Bitlocker - Windows 10 Pro & Executive)

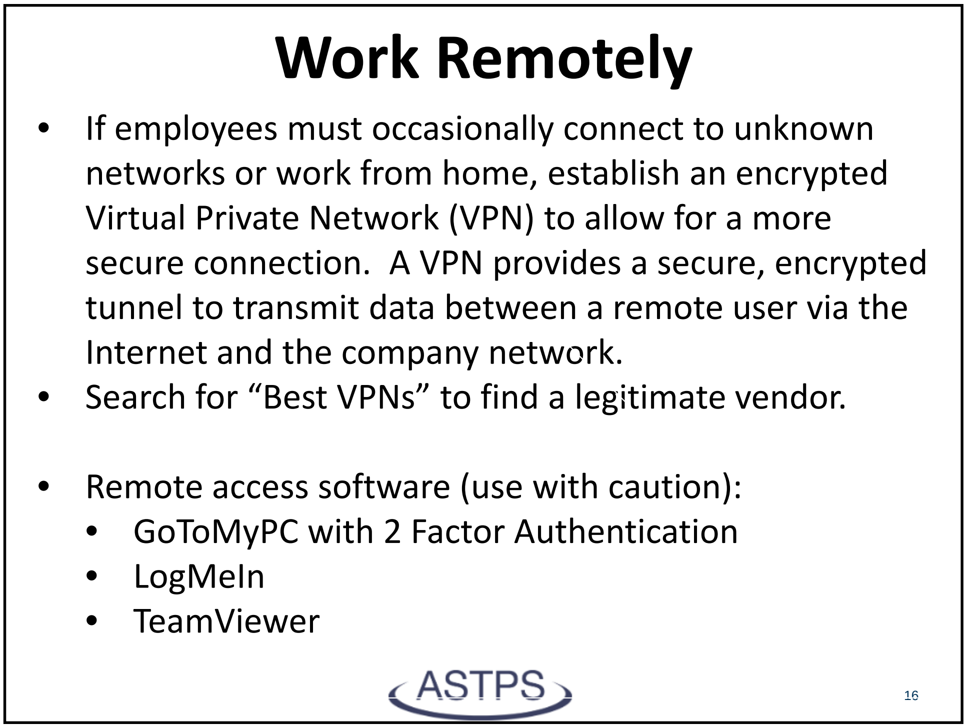


Secure Wireless Networks

- Change default administrative password of your wireless router – use a strong, unique password.
- Change the name of your router to something NOT personally identifiable (i.e., Bob'sTaxService) and disable the SSID (**S**ervice**S**et**ID**entifier) Broadcast so that it cannot be seen by those who have no need to use your network.
- Use Wi-Fi Protected Access 2 (WPA-2) with the advanced Encryption Standard (AES) for encryption.
- Do **NOT** use Wired-Equivalency Privacy (WEP).
- Do **NOT** use public Wi-Fi (airport, coffee shop) to access business e-Mails or Sensitive Documents.

ASTPS

15



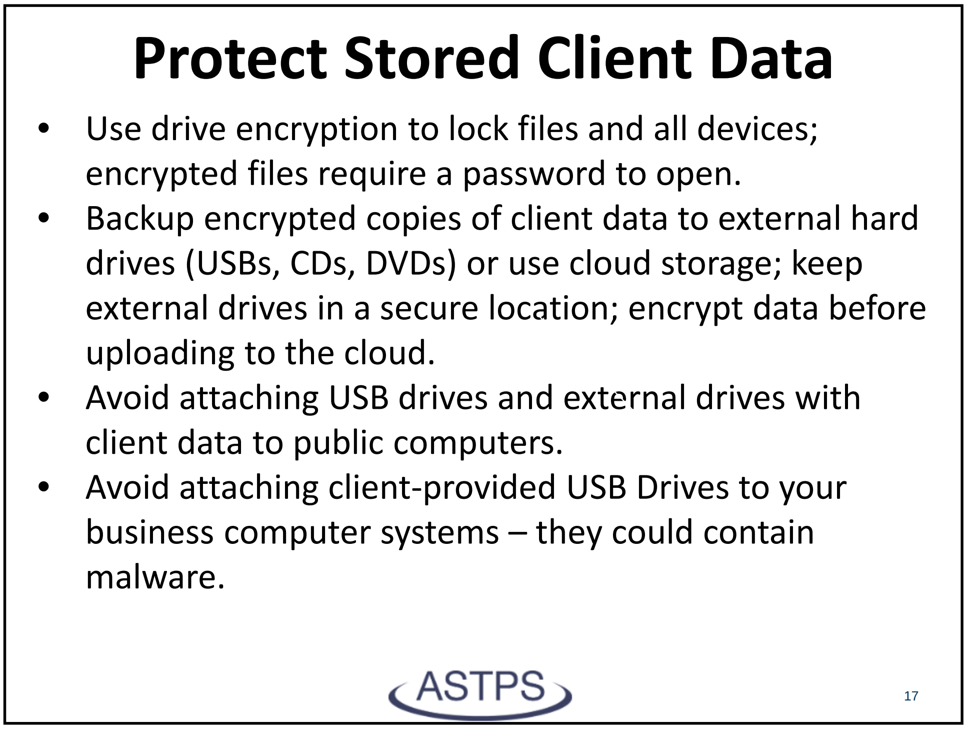
Work Remotely

- If employees must occasionally connect to unknown networks or work from home, establish an encrypted Virtual Private Network (VPN) to allow for a more secure connection. A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and the company network.
- Search for "Best VPNs" to find a legitimate vendor.

- Remote access software (use with caution):
  - GoToMyPC with 2 Factor Authentication
  - LogMeIn
  - TeamViewer

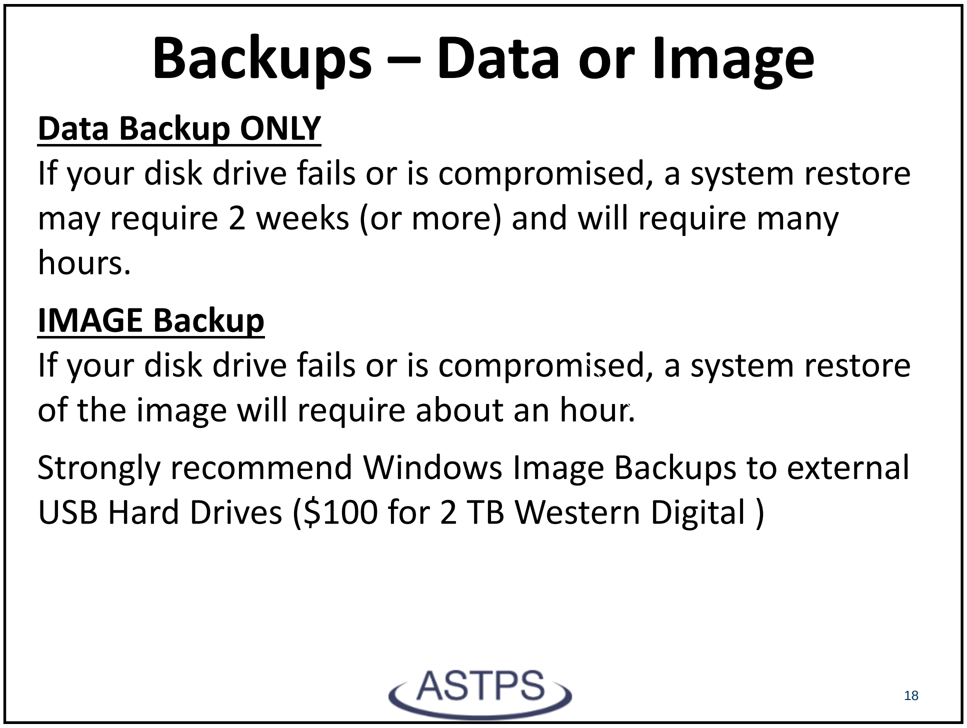
ASTPS

16



Protect Stored Client Data

- Use drive encryption to lock files and all devices; encrypted files require a password to open.
- Backup encrypted copies of client data to external hard drives (USBs, CDs, DVDs) or use cloud storage; keep external drives in a secure location; encrypt data before uploading to the cloud.
- Avoid attaching USB drives and external drives with client data to public computers.
- Avoid attaching client-provided USB Drives to your business computer systems – they could contain malware.



Backups – Data or Image

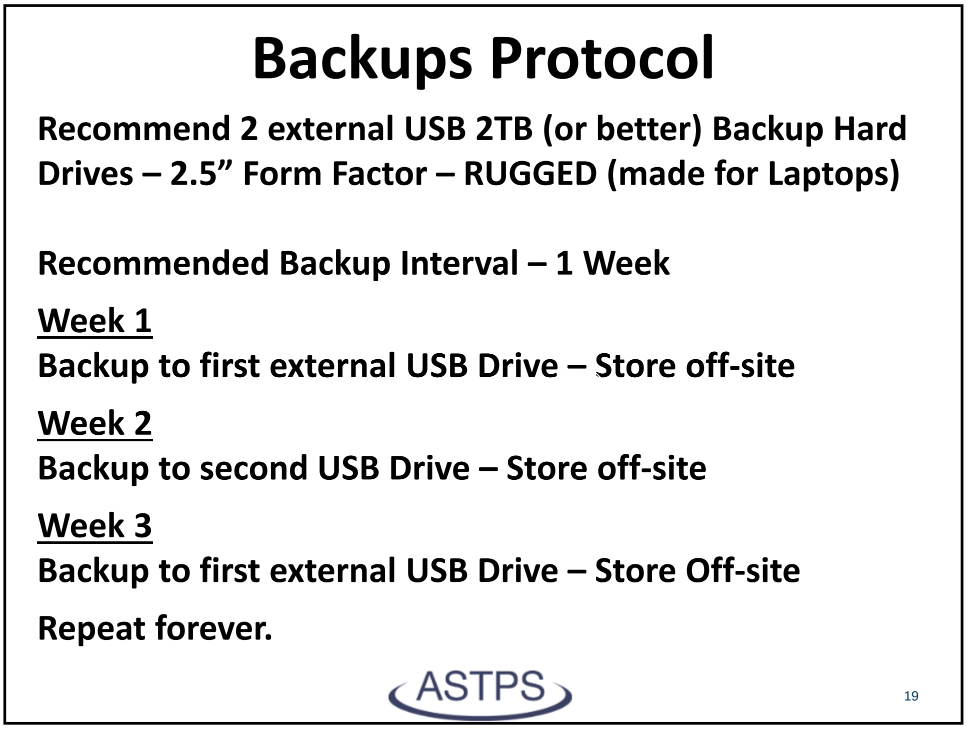
Data Backup ONLY

If your disk drive fails or is compromised, a system restore may require 2 weeks (or more) and will require many hours.

IMAGE Backup

If your disk drive fails or is compromised, a system restore of the image will require about an hour.

Strongly recommend Windows Image Backups to external USB Hard Drives ($100 for 2 TB Western Digital)



Backups Protocol

Recommend 2 external USB 2TB (or better) Backup Hard Drives – 2.5" Form Factor – RUGGED (made for Laptops)

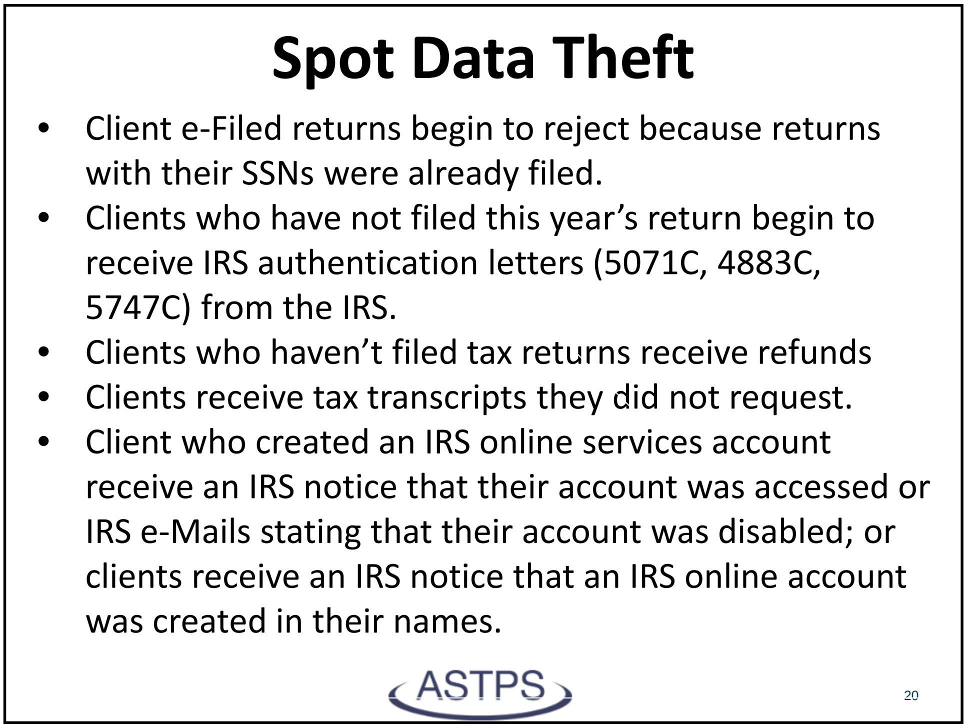
Recommended Backup Interval – 1 Week

<u>Week 1</u>
Backup to first external USB Drive – Store off-site

<u>Week 2</u>
Backup to second USB Drive – Store off-site

<u>Week 3</u>
Backup to first external USB Drive – Store Off-site

Repeat forever.



Spot Data Theft

- Client e-Filed returns begin to reject because returns with their SSNs were already filed.
- Clients who have not filed this year's return begin to receive IRS authentication letters (5071C, 4883C, 5747C) from the IRS.
- Clients who haven't filed tax returns receive refunds
- Clients receive tax transcripts they did not request.
- Client who created an IRS online services account receive an IRS notice that their account was accessed or IRS e-Mails stating that their account was disabled; or clients receive an IRS notice that an IRS online account was created in their names.

Spot Data Theft

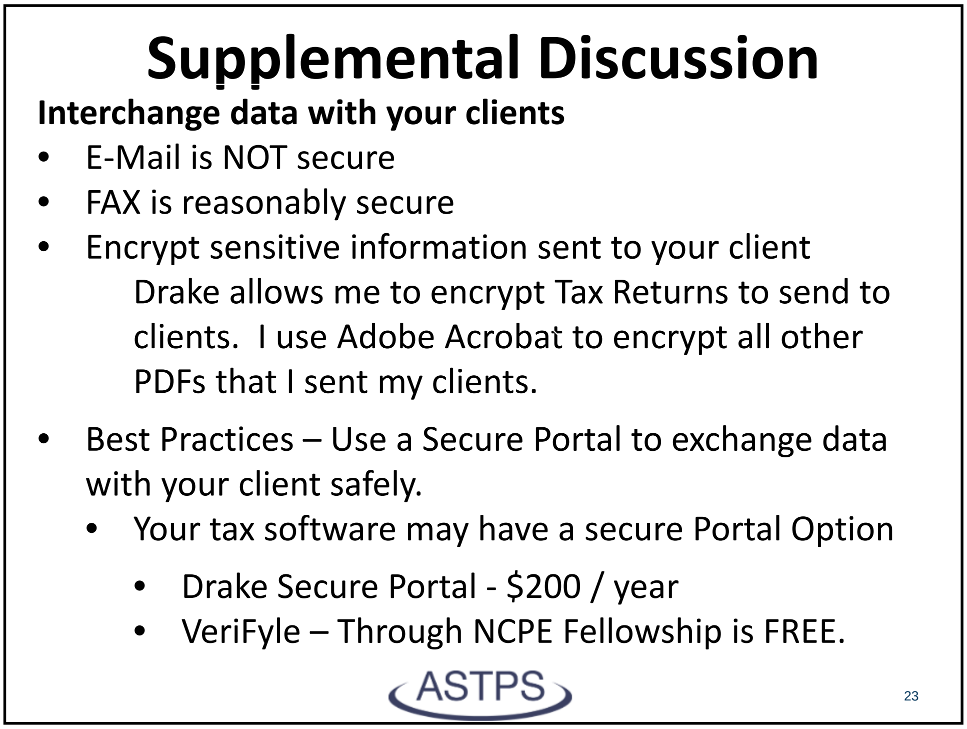
- The number of returns filed with tax practitioner's EFIN (Electronic Filing Identification Number exceeds the number of clients.
- Tax professionals or clients responding to e-Mails that the practitioners did NOT send.
- Computer cursor moving or changing numbers without touching the keyboard or mouse.
- Network computers locking out tax practitioners.

ASTPS

Monitor EFIN/PTINs Weekly

- Obtain a weekly report of the number of tax returns filed with your EFIN or your PTIN.
- Weekly checks will help flag any abuses
- Contact the IRS e-Help Desk if the return totals exceed the number of returns the tax professional filed.
- Excessive use or misuse of PTINs - Complete Form **14157 – Complaint: Tax Return Preparer**, to report excessive use or misuse of your PTIN.

ASTPS



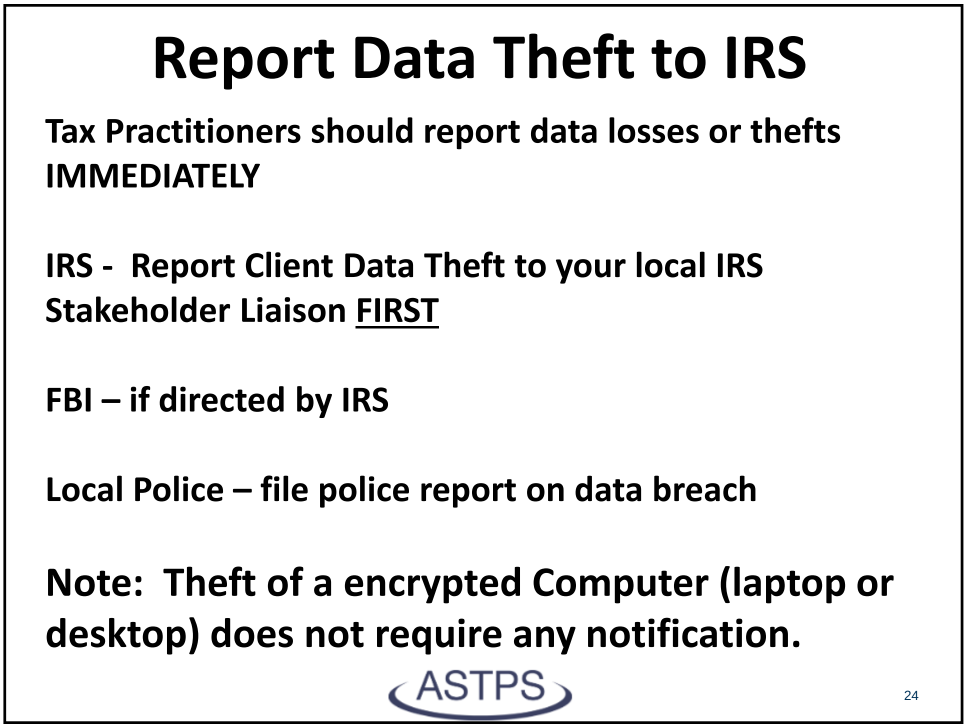
Supplemental Discussion

Interchange data with your clients

- E-Mail is NOT secure
- FAX is reasonably secure
- Encrypt sensitive information sent to your client

  Drake allows me to encrypt Tax Returns to send to clients. I use Adobe Acrobat to encrypt all other PDFs that I sent my clients.

- Best Practices – Use a Secure Portal to exchange data with your client safely.
  - Your tax software may have a secure Portal Option
    - Drake Secure Portal - $200 / year
    - VeriFyle – Through NCPE Fellowship is FREE.



Report Data Theft to IRS

Tax Practitioners should report data losses or thefts IMMEDIATELY

IRS - Report Client Data Theft to your local IRS Stakeholder Liaison FIRST

FBI – if directed by IRS

Local Police – file police report on data breach

Note: Theft of a encrypted Computer (laptop or desktop) does not require any notification.

Best Practices - Cyber Insurance

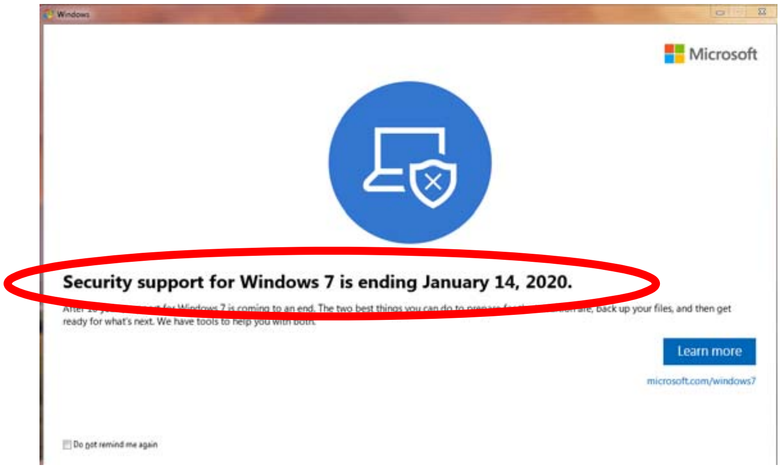
Data Breach can put you out of business.

Good idea to purchase Cyber Insurance.

ASTPS

Migrate to Windows 10 Soon

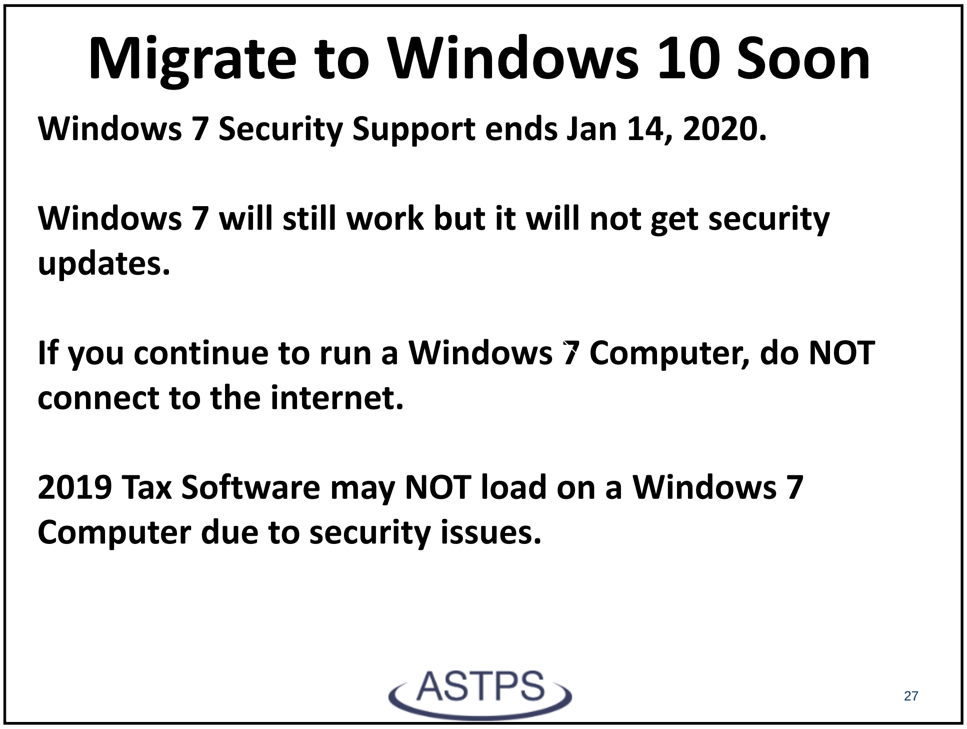
Windows 7 users are seeing the warning screen shown below.



Security support for Windows 7 is ending January 14, 2020.

After 10 years, support for Windows 7 is coming to an end. The two best things you can do to prepare for [illegible] are, back up your files, and then get ready for what's next. We have tools to help you with both.

ASTPS



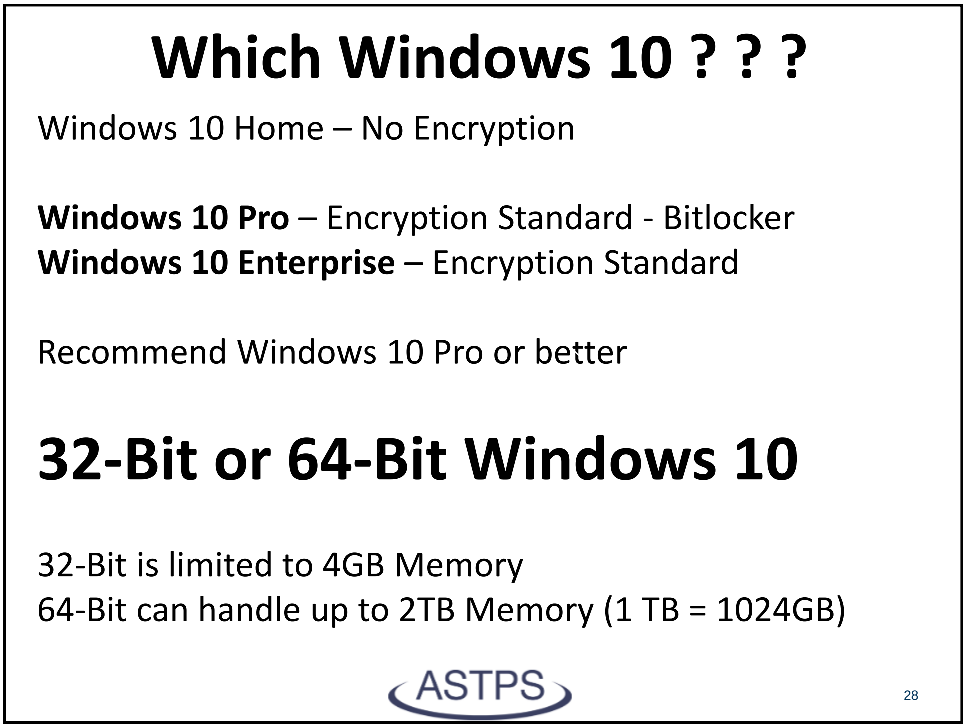
Migrate to Windows 10 Soon

Windows 7 Security Support ends Jan 14, 2020.

Windows 7 will still work but it will not get security updates.

If you continue to run a Windows 7 Computer, do NOT connect to the internet.

2019 Tax Software may NOT load on a Windows 7 Computer due to security issues.



Which Windows 10 ? ? ?

Windows 10 Home – No Encryption

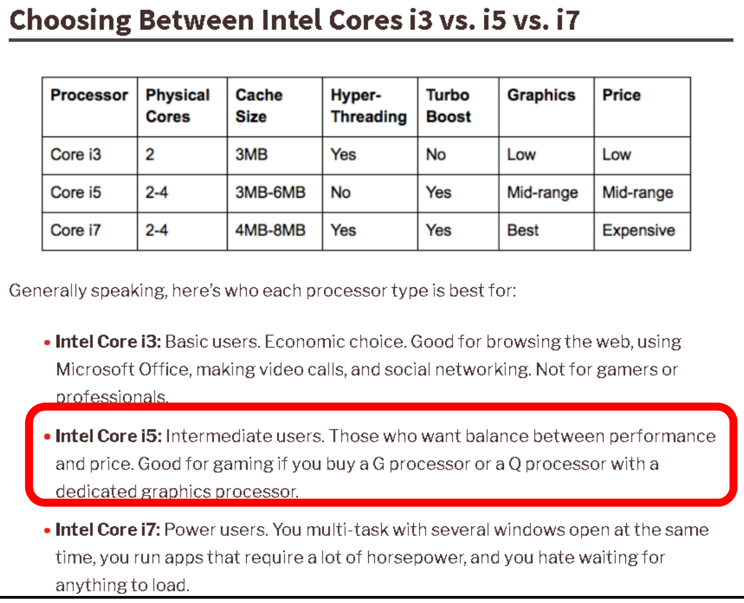
Windows 10 Pro – Encryption Standard - Bitlocker
Windows 10 Enterprise – Encryption Standard

Recommend Windows 10 Pro or better

32-Bit or 64-Bit Windows 10

32-Bit is limited to 4GB Memory
64-Bit can handle up to 2TB Memory (1 TB = 1024GB)

Which Intel Processor ? ? ?



Choosing Between Intel Cores i3 vs. i5 vs. i7

Processor	Physical Cores	Cache Size	Hyper-Threading	Turbo Boost	Graphics	Price
Core i3	2	3MB	Yes	No	Low	Low
Core i5	2-4	3MB-6MB	No	Yes	Mid-range	Mid-range
Core i7	2-4	4MB-8MB	Yes	Yes	Best	Expensive

Generally speaking, here's who each processor type is best for:

- **Intel Core i3:** Basic users. Economic choice. Good for browsing the web, using Microsoft Office, making video calls, and social networking. Not for gamers or professionals.
- **Intel Core i5:** Intermediate users. Those who want balance between performance and price. Good for gaming if you buy a G processor or a Q processor with a dedicated graphics processor.
- **Intel Core i7:** Power users. You multi-task with several windows open at the same time, you run apps that require a lot of horsepower, and you hate waiting for anything to load.

Recommended Windows 10

64-Bit Windows 10 Pro, 16GB, i5 Processor

Encryption Standard – Bitlocker
8GB Minimum RAM Memory – 16GB is better

Processor: i5 (reasonable performance)

Refurb Dell MiniTower prices start at $220-ish for 64-Bit Windows 10 Pro, i5, 16GB, 500GB SATA hard Drive.

Recently purchased a refurb 1TB Seagate SATA Drive - $40 with a 1-year warranty.

ASTPS

Data Security Plan is based on IRS Pub 4557

Page 1 Overview of Data Security Plan

Page 2 Computer Inventory

Page 3-6 4557 Safeguards Rule Checklist

Page 1 Overview of Data Security Plan

(Insert your Company Name Here) Data Security Plan Overview

Plan Administrator: Name
Cell XXX-XXX-XXXX
e-Mail

Physical Location of Office
XXXX Pleasantdale Rd **(Insert your Data)**
Atlanta, GA 30340

Mailing Address
Tax Doctor, Inc
3631 Chamblee Tucker Rd, A-316 **(Insert your Data)**
Atlanta, GA 30341

Internet Provider: (E.g. Comcast)
Router: your Router and model number

System administration and backup performed by (Name of Plan Administrator)

Page 2 is printout of Computer Inventory (File 2 is EXCEL Template)

Page 3 thru 6 is the Pub 4557 Safeguards Rule Checklist (Pages 14-17) with the appropriate check boxes completed by you.

Page 2 Computer Inventory

Computer Serial Numbers are important if your computer is stolen and you have to file a police report.

#	Image Backup	Create Restore Point	Computer Name	Description	Serial Number or Service Tag	Operating System	Encrypted	Anti Virus	Firewall
1	Weekly	Weekly	Server - Drake & Qbooks	Vision I5 64-Bit 8GB Front Office RAID Drives	CS-CM ELITE 2046563 RC342KKRJ1122500026	Windows 7 Pro	Symantec	AVG Free	Windows Firewall & Router
2	Weekly	Weekly	Merry's Computer	Vision I5 64-Bit 8GB Front Office RAID Drives	CS-CM ELITE 2046560 RC342KKRJ1123200239	Windows 7 Pro	Symantec	AVG Free	Windows Firewall & Router
3	Weekly	Weekly	Bill's Computer	Vision I5 64-Bit 8GB Front Office RAID Drives	CS-CM ELITE 2046561 RC342KKRJ1122199648	Windows 7 Pro	Symantec	Malware Bytes	Windows Firewall & Router
4	Weekly	Weekly	BASCORP	Dell GX-780 32-Bit 4GB	6V49KQ1	Windows 7 Pro	NO	AVG Free	Windows Firewall & Router
	Weekly	Weekly	Home	Dell GX-780 32-Bit 4GB	1TTS9P1	Windows 7 Pro	NO	Malware Bytes	Windows Firewall & Router

ASTPS

Page 3 thru 6
4557 Safeguards Rule Checklist

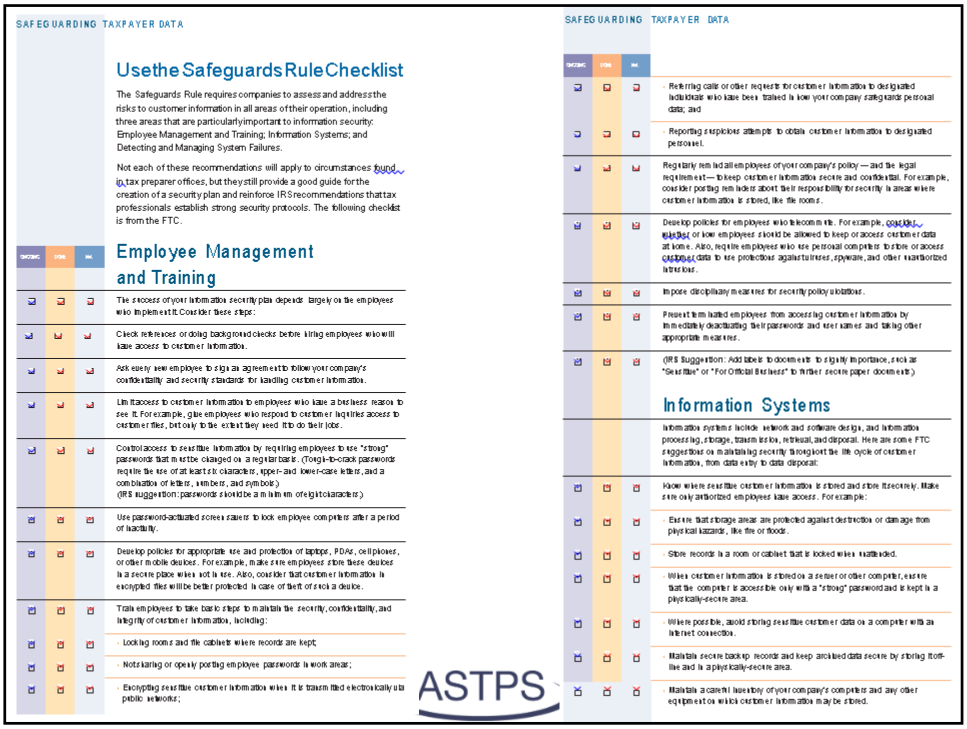
Usethe SafeguardsRuleChecklist

The Safeguards Rule requires companies to assess and addressthe risks to customer information in all areas of their operation, including three areas that are particularlyimportant to information security: Employee Management and Training; Information Systems; and Detecting and Managing System Failures.

Not each of these recommendations will apply to circumstances found in tax preparer offices, but theystill provide a good guide for the creation of a security plan and reinforce IRS recommendations that tax professionals establish strong security protocols. The following checklist is from the FTC.

Employee Management and Training

ONGOING	DONE	N/A	
☑	☑	☑	The success of your information security plan depends largely on the employees who implement it. Consider these steps:
☑	☑	☑	Check references or doing background checks before hiring employees who will have access to customer information.
☑	☑	☑	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.



Use the Safeguards Rule Checklist

The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operation, including three areas that are particularly important to information security: Employee Management and Training; Information Systems; and Detecting and Managing System Failures.

Not each of these recommendations will apply to circumstances found in tax preparer offices, but they still provide a good guide for the creation of a security plan and reinforce IRS recommendations that tax professionals establish strong security protocols. The following checklist is from the FTC.

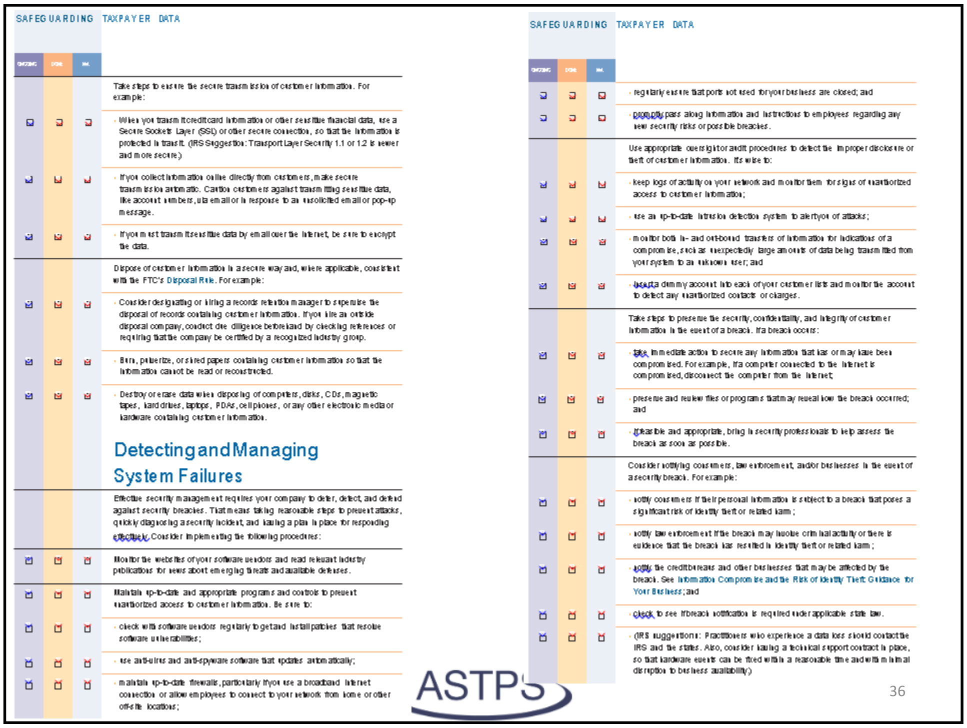
Employee Management and Training

ONGOING	DONE	N/A	
☑	☑	☑	The success of your information security plan depends largely on the employees who implement it. Consider these steps:
☑	☑	☑	Check references or doing background checks before hiring employees who will have access to customer information.
☑	☑	☑	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;

ONGOING	DONE	N/A	
☑	☑	☑	· 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 user names 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

ONGOING	DONE	N/A	
			Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some FTC suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal:
☑	☑	☑	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 off-line 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.



ONGOING	DONE	N/A	
			Take steps to ensure the secure transmission of customer information. For example:
☑	☑	☑	· 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. For example:
☑	☑	☑	· 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

ONGOING	DONE	N/A	
			Effective security management requires your company to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:
☑	☑	☑	Monitor the websites of your software vendors and read relevant industry publications for news about emerging threats and available defenses.
☑	☑	☑	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;

ONGOING	DONE	N/A	
☑	☑	☑	· regularly ensure that ports not used for your business are closed; and
☑	☑	☑	· 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. If a breach occurs:
☑	☑	☑	· take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet;
☑	☑	☑	· preserve and review files or programs that may reveal how the breach occurred; and
☑	☑	☑	· if feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.
			Consider notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example:
☑	☑	☑	· notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm;
☑	☑	☑	· notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;
☑	☑	☑	· notify the credit bureaus and other businesses that may be affected by the breach. See Information Compromise and the Risk of Identity Theft: Guidance for Your Business; and
☑	☑	☑	· check to see if breach notification is required under applicable state law.
☑	☑	☑	· (IRS suggestions: Practitioners who experience a data loss should contact the IRS and the states. Also, consider having a technical support contract in place, so that hardware events can be fixed within a reasonable time and with minimal disruption to business availability.)

Templates to Generate YOUR Data Security Plan are available using Drake Secure Portal.

- <u>**Access the Security Data Plan via Drake Secure File Pro**</u>
- Enter the following in your browser:

TaxAuditGuardian.SecureFilePro.com

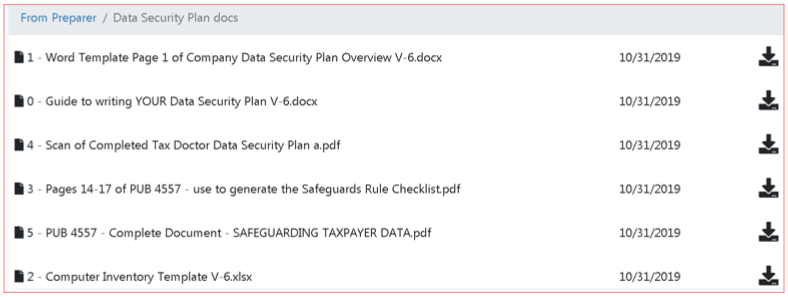
User Name: GAEAmember
Password: gaea2019

ASTPS

Click on Data Security Plan docs - You get the Screen shown below:

Download each file to a folder on your computer.

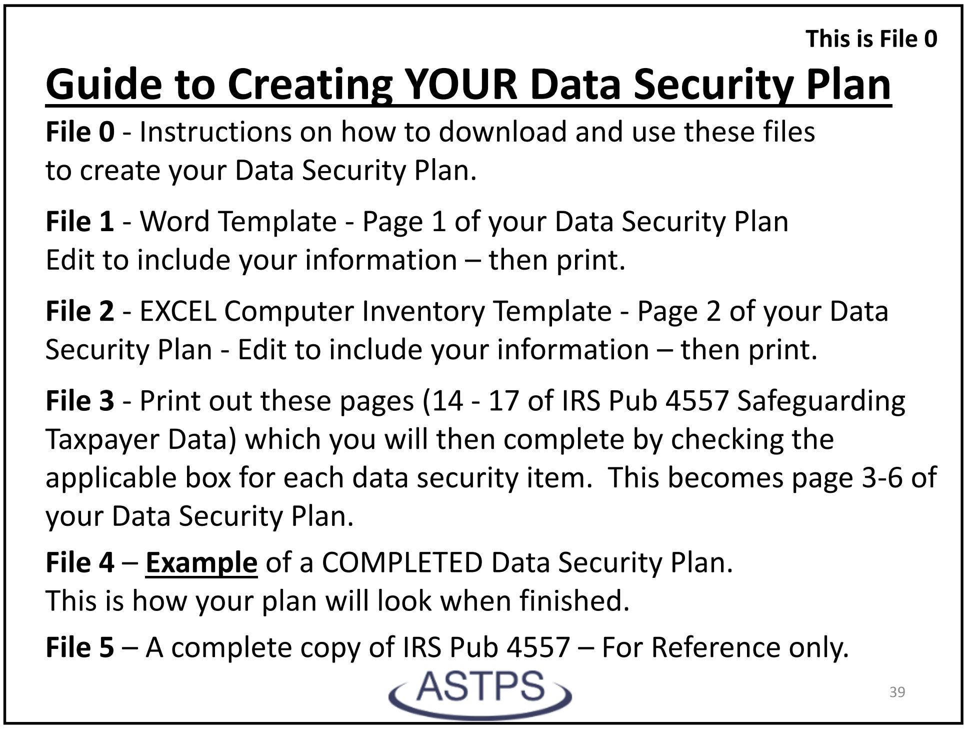
Click on the Download Icon ⬇ to download and store each file.



From Preaparer / Data Security Plan docs

1 - Word Template Page 1 of Company Data Security Plan Overview V-6.docx	10/31/2019	⬇
0 - Guide to writing YOUR Data Security Plan V-6.docx	10/31/2019	⬇
4 - Scan of Completed Tax Doctor Data Security Plan a.pdf	10/31/2019	⬇
3 - Pages 14-17 of PUB 4557 - use to generate the Safeguards Rule Checklist.pdf	10/31/2019	⬇
5 - PUB 4557 - Complete Document - SAFEGUARDING TAXPAYER DATA.pdf	10/31/2019	⬇
2 - Computer Inventory Template V-6.xlsx	10/31/2019	⬇

Open File 0 – Guide to writing YOUR Data Security Plan and follow the instructions.



This is File 0

Guide to Creating YOUR Data Security Plan

File 0 - Instructions on how to download and use these files to create your Data Security Plan.

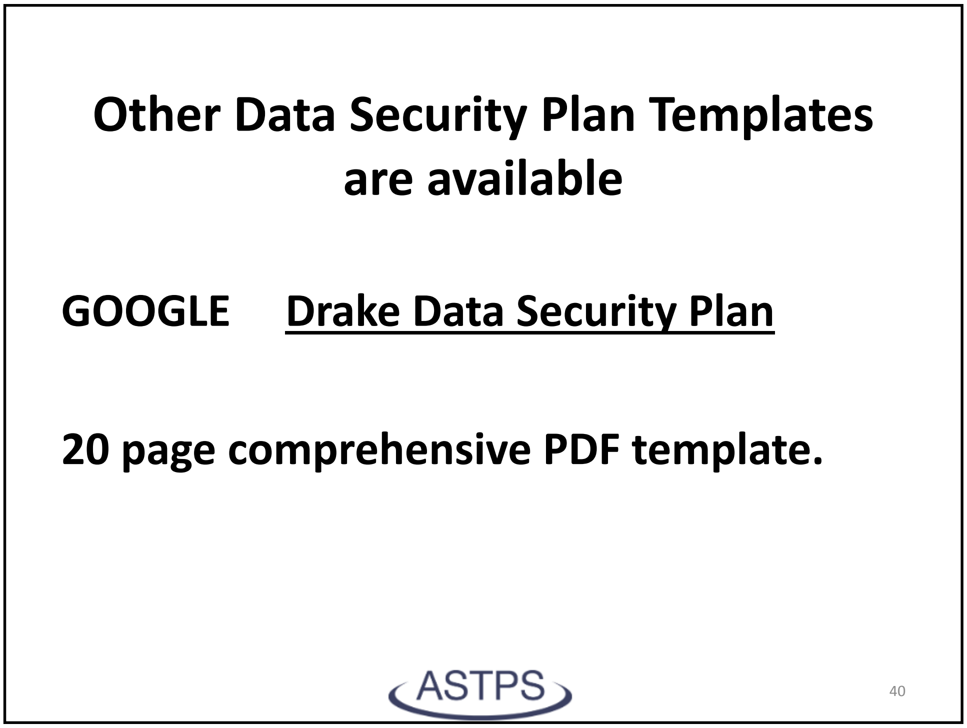
File 1 - Word Template - Page 1 of your Data Security Plan Edit to include your information – then print.

File 2 - EXCEL Computer Inventory Template - Page 2 of your Data Security Plan - Edit to include your information – then print.

File 3 - Print out these pages (14 - 17 of IRS Pub 4557 Safeguarding Taxpayer Data) which you will then complete by checking the applicable box for each data security item. This becomes page 3-6 of your Data Security Plan.

File 4 – **Example** of a COMPLETED Data Security Plan. This is how your plan will look when finished.

File 5 – A complete copy of IRS Pub 4557 – For Reference only.



Other Data Security Plan Templates are available

GOOGLE Drake Data Security Plan

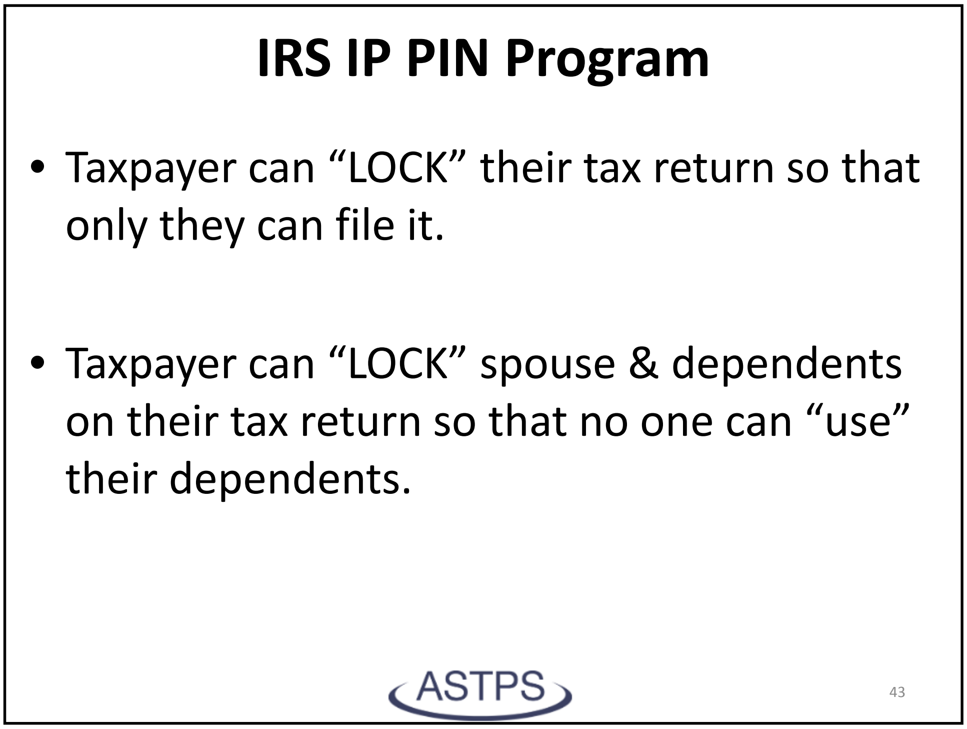
20 page comprehensive PDF template.

Suggested Best Practices

- Recommend your client "LOCK" or "FREEZE" their Tax Return (via IRS IP PIN program). No one else can file a return using their name and SSN.
- Recommend your client put a Fraud Alert or Credit Freeze on their financial accounts.
- Significant Data Breaches have occurred over the last 5 years.

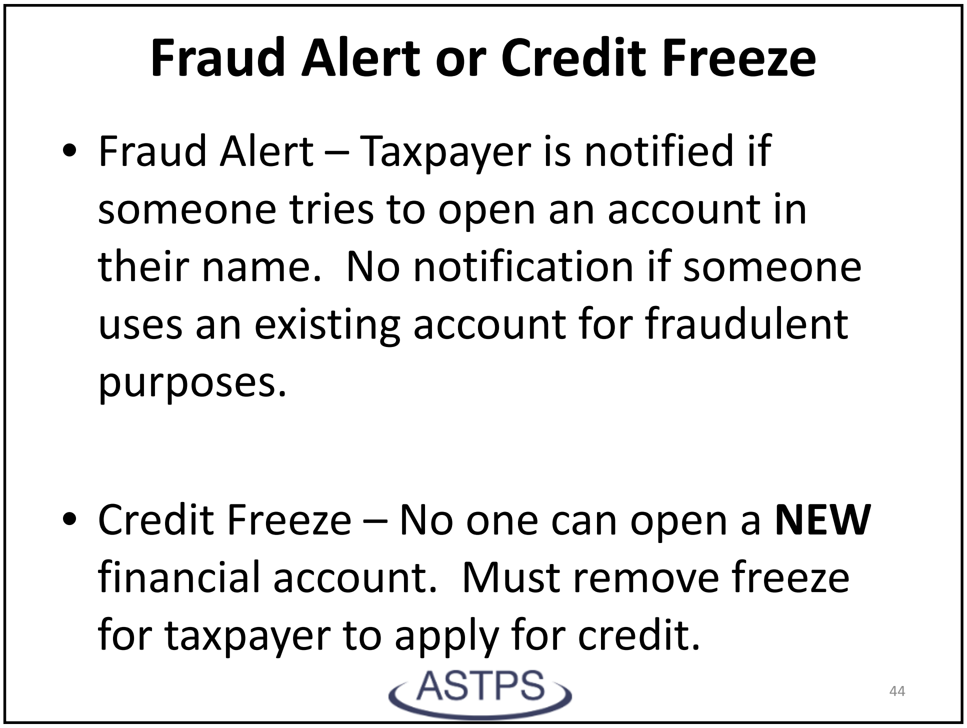
IRS IP PIN Program

- If you live in one of 20 states listed below, you are eligible for the online IP PIN Opt-In Program.
- You must have filed a federal return last year as a resident of Arizona, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, New York, North Carolina, Pennsylvania, Rhode Island, Texas or Washington.
- IRS is planning on rolling out this program nationally.



IRS IP PIN Program

- Taxpayer can “LOCK” their tax return so that only they can file it.
- Taxpayer can “LOCK” spouse & dependents on their tax return so that no one can “use” their dependents.



Fraud Alert or Credit Freeze

- Fraud Alert – Taxpayer is notified if someone tries to open an account in their name. No notification if someone uses an existing account for fraudulent purposes.
- Credit Freeze – No one can open a **NEW** financial account. Must remove freeze for taxpayer to apply for credit.

Fraud Alert

- Recommend that your clients put a fraud alert on their financial information.
- Can place a Fraud Alert on-line with one of the credit bureaus. That credit bureau notifies the others AUTOMATICALLY.
- NO Charge ! !

Questions ? ? ?

Bill Nemeth, EA
WGNemeth@aol.com
Cell: 770-616-1638