Safeguarding Taxpayer Data

A Guide for Your Business

IRS

Department of the Treasury
Internal Revenue Service

www.irs.gov

Publication 4557 (10-2006)
Catalog Number 48905Y

Contents

1. The Need to Safeguard Taxpayer Data

Safeguarding taxpayer data is a top priority for the IRS. It is the responsibility of government, businesses, organizations, and individuals that receive, maintain, share, transmit, or store taxpayers' personal information. Taxpayer data is defined as any information that is obtained or used in the preparation of a tax return (e.g., income statements, notes taken in a meeting, or recorded conversations). Whether you are paid or unpaid for your services, a one person operation or a large corporation, have one client or thousands, it is critical to protect taxpayer data. Putting safeguards in place helps prevent fraud and identity theft, and enhances customer confidence and trust.

This guide will help non-governmental businesses, organizations, and individuals that handle taxpayer data to understand and meet their responsibility to safeguard this information. IRS *e-file* and paper Return Preparers, Intermediate Service Providers, Software Developers, Electronic Return Originators, Reporting Agents, Transmitters, their affiliates, and service providers can use this guide to determine and meet their data privacy and security needs.

There are a growing number of laws, regulations, standards, and best practices that cover the privacy and security of taxpayer data. This guide references those that provide guidelines on establishing safeguards that help you:

- Preserve the confidentiality and privacy of taxpayer data by restricting access and disclosure,
- Protect the integrity of taxpayer data by preventing improper or unauthorized modification or destruction, and
- Maintain the availability of taxpayer data by providing timely and reliable access and data recovery.

For a brief description of related laws and regulations, refer to the table in Chapter 4, "Safeguarding Taxpayer Data, References to Applicable Laws and Regulations." For references to standards and best practices, refer to the table in Chapter 5, "Safeguarding Taxpayer Data, References to Applicable Standards and Best Practices."

Bert W. DuMars
Director, Electronic Tax Administration

Richard J. Morgante

Richard J. Morgante
Commissioner, Wage & Investment Division

2. How to Safeguard Taxpayer Data

Getting Started

If you handle taxpayer data and are paid for your services, you are subject to the Federal Trade Commission (FTC) Privacy and Safeguards Rules. Whether or not you are subject to the FTC Rules, and whether or not you are paid for your services, you will benefit from implementing the general processes and best practices outlined in several of their documents.

Financial institutions as defined by FTC include professional tax preparers, data processors, their affiliates, and service providers who are paid for their services. They must take the following steps to protect taxpayer data. Other businesses, organization, and individuals handling taxpayer data should also follow these steps because they represent best practices for all.

- ➢ Take responsibility or assign an individual or individuals to be responsible for safeguards,
- ➢ Assess the risks to taxpayer data in your office, including your operations, physical environment, computer systems, and employees if applicable. Make a list of all the locations you keep taxpayer information (computers, filing cabinets, bags, and boxes taxpayers may bring you),
- ➢ Write a plan of how you will safeguard taxpayer data. Put appropriate safeguards in place,
- ➢ Use only service providers who have policies in place to also maintain an adequate level of information protection defined by the Safeguards Rule, and
- ➢ Monitor, evaluate, and adjust your security program as your business or circumstances change.

The FTC has fact sheets and guidelines on privacy and safeguards for businesses on their website at www.ftc.gov. In addition, you may seek outside professional help to assess your security needs.

To safeguard taxpayer data, you must determine the appropriate security controls for your environment based on the size, complexity, nature, and scope of your activities. Security controls are the management, operational, and technical safeguards you may use to protect the confidentiality, integrity, and availability of your customers' data. Examples of security controls are 1) locking doors to restrict access to paper or electronic files, 2) requiring passwords to restrict access to computer files, 3) encrypting electronically stored taxpayer data, 4) keeping a backup of electronic data for recovery purposes, and 5) shredding paper containing taxpayer data before throwing it in the trash. For additional examples of security controls, refer to the National Institute of Standards and Technology (NIST) SP 800-53 publication listed in Chapter 5.

Putting Safeguards in Place

The following checklist includes many activities that can be included in an information security program. It can help you put in place security procedures and controls to protect taxpayer data. It is important to consider all the safeguards that are applicable to your business.

Checklist for Safeguarding Taxpayer Data			
Administrative Activities	Ongoing	Done	N/A
Complete a Risk Assessment. Identify the risks and potential impacts of unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that can be used to access taxpayer data. How vulnerable is your customer's data to theft, disclosure, unauthorized alterations, or unrecoverable loss? What can you do to reduce the impact to your customers and your business in such an event? What can you do to reduce vulnerability?	□	□	
Write and follow an Information Security Plan that:	□	□	
Addresses every item identified in the risk assessment.	□	□	
Defines safeguards you want affiliates and service providers to follow.	□	□	
Requires a responsible person to review and approve the Information Security Plan.	□	□	
Requires a responsible person to monitor, revise, and test the Information Security Plan on a periodic (recommended annual) basis to address any system or business changes or problems identified.	□	□	
Periodically (recommended annually) perform a Self-Assessment to:	□	□	
Evaluate and test the security plan and other safeguards you have in place.	□	□	
Document information safeguards deficiencies. Create and execute a plan to address them.	□	□	
Retain a copy of the Self-Assessment and ensure it is available for any potential reviews.	□	□	
If required by the FTC Privacy Rule, provide privacy notices and practices to your customers.	□	□	□
Specify in contracts with service providers the safeguards they must follow and monitor how they handle taxpayer data.	□	□	□
Ask service providers to give you a copy of their written security policy on safeguarding data.	□	□	□
Facilities Security	Ongoing	Done	N/A
Protect from unauthorized access and potential danger (e.g., theft, floods, and tornados) all places where taxpayer data are located.	□	□	

Checklist for Safeguarding Taxpayer Data			
Write procedures that prevent unauthorized access and unauthorized processes.	□	□	
Assure that taxpayer data, including hardware and media, is not left un-secured on desks or photocopiers, in mailboxes, vehicles, trash cans, or rooms in the office or at home where unauthorized access can occur.	□	□	
Authorize and control delivery and removal of all taxpayer data, including hardware and media.	□	□	
Lock doors to file rooms and/or computer rooms.	□	□	
Provide secure disposal of taxpayer data, such as shredders, burn boxes, or temporary file areas until it can be securely disposed.	□	□	
Personnel Security	Ongoing	Done	N/A
Create and distribute Rules of Behavior that describe responsibilities and expected behavior regarding computer information systems as well as paper records and usage of taxpayer data. Have all information system users complete, sign, and submit an acknowledgement that they have read, understood, and agree to comply with the rules of behavior. An example of rules of behavior can be found in Appendix A of NIST SP-800 18 *Guide for Developing Security Plans for Information Technology Systems*, February 2006.	□	□	□
Ensure personnel from third-party providers such as service bureaus, contractors, and other businesses providing information technology services meet the same security requirements as those applied to your personnel.	□	□	□
Address Rules of Behavior for computer system management.	□	□	□
When interviewing prospective personnel, explain the expected Rules of Behavior.	□	□	□
When possible, perform a background and/or reference check on new employees who will have contact with taxpayer information. Conduct background screenings that are appropriate to the sensitivity of an assigned position.	□	□	□
Screen personnel prior to granting access to any paper or electronic data. This will help ensure their suitability for a position requiring confidentiality and trust.	□	□	□
Have personnel who will have access to taxpayer data sign nondisclosure agreements on the use of confidential taxpayer data.	□	□	□
Develop and enforce formal compliance policies and processes, including possible disciplinary action, for all personnel who do not comply with the businesses' established information security policies and procedures.	□	□	□
Terminate access to taxpayer data (e.g., login IDs and passwords) for those employees who are terminated or who no longer need to access taxpayer data.	□	□	□

Checklist for Safeguarding Taxpayer Data			
For each employee who is terminated, conduct an exit interview and ensure the employee returns property that allows access to taxpayer data (e.g., laptops, media, keys, identification cards, and building passes).	□	□	□
Train staff on Rules of Behavior for access, non-disclosure, and safeguards of taxpayer data. Provide refresher training periodically.	□	□	□
Information Systems Security	Ongoing	Done	N/A
Information systems include both automated and manual systems made up of people, machines, and/or methods for collecting, processing, transmitting, storing, archiving, and distributing data. To help ensure the accuracy, validity, consistency, and reliability of taxpayer data, you should manage taxpayer data information systems based on the guidelines below.			
Grant access to taxpayer data systems only on a valid need-to-know basis that is determined by the individual's role within the business.	□	□	
Put in place a written contingency plan to perform critical processing in the event that your business is disrupted. It should include a plan to protect both electronic and paper taxpayer data systems. Identify individuals who will recover and restore the system after disruption or failure.	□	□	
Periodically test your contingency plan.	□	□	
Back up taxpayer data files regularly (e.g., daily or weekly) and store backup information at a secure location.	□	□	□
Maintain hardware and software as needed and keep maintenance records.	□	□	□
Computer Systems Security	Ongoing	Done	N/A
Identify and authenticate computer system users who require access to electronic taxpayer data systems before granting them access. You can manage user identities by:	□	□	□
Identifying authorized users of electronic taxpayer data systems and grant specific access rights/privileges.	□	□	□
Assigning each user a unique identifier.	□	□	□
Verifying the identity of each user.	□	□	□
Disabling user identifiers after an organization-defined time period of inactivity.	□	□	□
Archiving user identities.	□	□	□
Implement password management procedures that require strong passwords. See the "Stop. Think. Click: Seven Practices for Safer Computing" reference listed in Chapter 5 for information on strong passwords.	□	□	□
Require periodic password changes.	□	□	□

Checklist for Safeguarding Taxpayer Data			
Disable and remove inactive user accounts.	□	□	□
Protect electronic taxpayer data systems connected to the Internet with a barrier device (e.g., firewall, router, or gateway). Any failure of these devices should not result in an unauthorized release of taxpayer data.	□	□	□
When storing taxpayer data electronically, consider following best practices and store it on separate secure computers or media that are not connected to a network and that are password protected and encrypted.	□	□	□
Encrypt taxpayer data when attached to email.	□	□	□
Encrypt taxpayer data when transmitting across networks.	□	□	□
Regularly update firewall, intrusion detection, anti-spyware, anti-adware, anti-virus software, and security patches.	□	□	□
Monitor computer systems for unauthorized access by reviewing system logs.	□	□	□
Lock out computer system users after three consecutive invalid access attempts.	□	□	□
Remove all taxpayer data once the retention period expires by using software designed to securely remove data from computers and media prior to disposing of hardware or media. The FTC Disposal Rule has information on how to dispose of sensitive data.	□	□	□
As recommended by the FTC, reduce risks to computer systems by performing vulnerability scans and penetration tests periodically. You can learn more about this at the FTC website in their article “FTC Facts for Business -- Security Check: Reducing Risks to Your Computer Systems.”	□	□	□
Media Security	Ongoing	Done	N/A
Store computer disks, removable media, tapes, compact disks, flash drives, audio and video recordings of conversations and meetings with taxpayers, and paper documents in a secure location, cabinet, or container.	□	□	
Secure media storage areas, including rooms, cabinets, and computers by locks or key access. Where appropriate, employ an automated mechanism to ensure only authorized access.	□	□	
Restrict authorized access to media storage.	□	□	
Limit removal of taxpayer data to authorized persons and perform data access audits regularly.	□	□	
Securely remove all taxpayer data when disposing of computers, diskettes, magnetic tapes, hard drives, or any other electronic media that contain taxpayer data. The FTC Disposal Rule has information on how to dispose of sensitive data.	□	□	
Shred or burn paper documents before discarding them.	□	□	

Checklist for Safeguarding Taxpayer Data

Certifying Information Systems for Use	Ongoing	Done	N/A
Determine if risks are acceptable to certify systems for use.	□	□	□
Sign an authority to operate.	□	□	□
If you use a certified independent certification company, consider the following:	□	□	□
On a periodic (recommended annual) basis, have an independent individual or business with relevant security expertise, evaluate the security plans, controls, and any other safeguards implemented in your business against best practices.	□	□	
Have a report generated from the audit that certifies that your business follows best practices.	□	□	
Ensure the report highlights any deficiencies and provides recommendations for their correction.	□	□	
Develop a plan for your business to correct any deficiencies found and to ensure that the plan is successfully executed.	□	□	
Retain a copy of the audit report to ensure it is available for any potential reviews.	□	□	
Be prepared to show how you mitigate risks.	□	□	

3. Reporting Incidents

Safeguarding personally identifiable taxpayer data is of critical importance to retaining the confidence and trust of taxpayers. If you believe a data security breach has occurred that affects the confidentiality, integrity, or availability of taxpayer data or the ability for the taxpayer to prepare or file a return, we recommend that you report the incident. An incident is a breach involving an unauthorized disclosure, misuse, modification, or destruction of taxpayer data. Incident types include the following:

Incident Type	Description
Unauthorized Access	A person or computer gains logical or physical access without permission to a network, system, application, data, or other resource.
Unauthorized Disclosure/ Usage	A person violates disclosure or use policies such as IRC sections 6713 & 7216. See Chapter 4, Laws and Regulations, for information on IRC sections 6713 & 7216.
Theft	Unauthorized removal of computers, data/records on computer media or paper files.
Loss/Accident	Accidental misplacement or loss of computers, data/records on computer media or paper files.
Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.
Denial of Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

The following are recommended actions for incident reporting:

- Individuals (e.g., employees and contractors) who detect a situation that may be a security incident should immediately inform the individual designated by the business to be responsible for handling customer data security.

- The individual responsible for handling customer data security should gather information about the suspected incident. We recommend that you consider reporting the incident to the IRS. The IRS may need to work closely with your business to quickly respond to incidents.

  To report the incident to IRS, at the IRS.gov website, select the "Contact IRS" link. Then select the "Contact the IRS.gov Help Desk" link. You may call IRS at 1-800-829-1040. The IRS contact may need to coordinate a response to the incident, working with your business and additional groups as needed to achieve resolution of the incident. This may include the Federal Trade Commission (FTC), the U.S. Treasury Inspector General for Tax Administration (TIGTA), IRS Criminal Investigations, IRS Computer Security Incident Response Center (CSIRC), IRS Taxpayer Advocate Service, IRS Office of Professional Responsibility, IRS Small Business/Self-Employed Business Operating Division, and/or the IRS Office of Identity Theft.

- If you believe the incident compromises a person's identity or their personal or financial information, we also recommend you refer to the FTC document, Information Compromise and the Risk of Identity Theft: Guidance for Your Business. Among other things, this reference will help you determine when to notify law enforcement. See the "Safeguarding Taxpayer Data, References to Applicable Standards and Best Practices" table in Chapter 5 for the Internet link to this FTC document.

4. Laws and Regulations

Many federal, state, city, and local government laws and regulations are in place to safeguard taxpayer data. The following table includes a brief description of some of them and provides references to more detailed information.

SAFEGUARDING TAXPAYER DATA REFERENCES TO APPLICABLE LAWS AND REGULATIONS	
Type	**Summary**
Federal/ Privacy & Security	The Gramm-Leach-Bliley Financial Modernization Act of 1999 – This statute (otherwise known as the Gramm-Leach-Bliley Act) (GLB Act), among other things, directed FTC to establish the Financial Privacy Rule and the Safeguards Rule. More information is available at http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.
Federal/ Privacy	*FTC Privacy of Consumer Financial Information Rule* (16 CFR Part 313) – This Rule (otherwise known as the Privacy Rule) aims to protect the privacy of the consumer by requiring financial institutions, as defined, which includes ***professional tax preparers, data processors, affiliates, and service providers who are paid for their services***, to give their customers privacy notices that explain the financial institution's information collection and sharing practices. In turn, customers have the right to limit some sharing of their information. Also, financial institutions and other companies that receive personal financial information from a financial institution may be limited in their ability to use that information. The FTC Privacy Rule implements sections 501 and 502(b)(2) of the GLB Act requirements. The Privacy Rule is available at http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html.
Federal/ Security	*FTC Standards for Safeguarding Customer Information Rule* (16 CFR Part 314)– This Rule (otherwise known as the Safeguards Rule) requires financial institutions, as defined, which includes ***professional tax preparers, data processors, affiliates, and service providers who are paid for their services***, to ensure the security and confidentiality of customer records and information. It protects against any anticipated threats or hazards to the security or integrity of such records. In addition, it protects against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. This Rule requires that financial institutions develop, implement, and maintain an Information Security Program. The plan should be written in one or more accessible parts and contain administrative, technical, and physical safeguards that are appropriate to the business' size and complexity, nature and scope of activities, and sensitivity of customer information handled. The Safeguards Rule is available at http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.
Federal/ Privacy	*Internal Revenue Code (IRC) section 7216* – This provision imposes criminal penalties on ***any person engaged in the business of preparing or providing services in connection with the preparation of tax returns*** who knowingly or recklessly makes unauthorized disclosures or uses of information furnished to them in connection with the preparation of an income tax return. A copy of Internal Revenue Code (IRC) section 7216 is available at http://www4.law.cornell.edu/uscode/html/uscode26/usc_sec_26_00007216----000-.html.

<table>
<tr><th colspan="2">SAFEGUARDING TAXPAYER DATA
REFERENCES TO APPLICABLE LAWS AND REGULATIONS</th></tr>
<tr><th>Type</th><th>Summary</th></tr>
<tr><td>Federal/ Privacy</td><td><i>Internal Revenue Code (IRC) section 6713</i> – This provision imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by <b><i>any person engaged in the business of preparing or providing services in connection with the preparation of tax returns</i></b>. A copy of Internal Revenue Code (IRC) section 6713 is available at http://www4.law.cornell.edu/uscode/html/uscode26/usc_sec_26_00006713----000-.html.</td></tr>
<tr><td>Federal/ Privacy</td><td><i>Internal Revenue Procedure 2005-60</i> – This procedure requires <b><i>Authorized IRS e-file Providers</i></b> to have security systems in place to prevent unauthorized access to taxpayer accounts and personal information by third parties. It also specifies that violations of the GLB Act and the implementing rules and regulations promulgated by the FTC, as well as violations of the non-disclosure rules contained in IRC sections 6713 and 7216 are considered violations of Revenue Procedure 2005-60, and are subject to sanctions specified in the Revenue Procedure. A copy of Internal Revenue Procedure 2005-60 is available at http://www.irs.gov/irb/2005-60_IRB/ar20.html.</td></tr>
<tr><td>Federal/ Security</td><td><i>Sarbanes-Oxley Act of 2002</i> (17 CFR Parts 232, 240 and 249) – Section 404 requirements apply to all <b><i>Securities and Exchange Commission (SEC) reporting companies</i></b> with a market capitalization in excess of $75 million. It requires companies to establish an infrastructure to protect and preserve records and data from destruction, loss, unauthorized alteration, or other misuse. This infrastructure must ensure there is no room for unauthorized alteration of records vital to maintaining the integrity of the business processes. More information is at http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf.</td></tr>
<tr><td>State/ Privacy & Security</td><td><i>State Laws</i> – Many state laws govern or relate to the privacy and security of financial data, which includes taxpayer data. They extend rights and remedies to consumers by requiring individuals and businesses that offer financial services to safeguard nonpublic personal information. For more information on state laws that <b><i>your business</i></b> must follow, consult state laws and regulations.</td></tr>
</table>

5. Standards and Best Practices

Federal and state governments as well as private industry provide many data security standards and best practice guidelines to safeguard consumer information such as personal tax data. The National Institute of Standards and Technology (NIST) provides security guidelines and practices for federal agencies that nongovernmental organizations may also use. Below is a list of references on a variety of safeguard topics that can help you comply with laws, regulations, and best practices that may apply to your business.

SAFEGUARDING TAXPAYER DATA REFERENCES TO APPLICABLE STANDARDS AND BEST PRACTICES	
Type	**Reference**
Federal/ Privacy	*"Getting Noticed: Writing Effective Financial Privacy Notices"* http://www.ftc.gov/privacy/privacyinitiatives/safeguards_educ.html
Federal/ Privacy	*"Information Compromise and the Risk of Identity Theft: Guidance for Your Business"* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.htm
Federal/ Security	*"FTC Facts for Business: Financial Institutions and Customer Information: Complying with the Safeguards Rule"* http://www.ftc.gov/privacy/privacyinitiatives/safeguards_educ.html
Federal/ Security	*FTC Disposal Rule (2005) -- "FTC Business Alert: Disposing of Consumer Report Information? New Rules Tell How"* http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.html
Federal/ Security	*"Security Check: Reducing Risks to Your Computer Systems"* http://www.ftc.gov/privacy/privacyinitiatives/safeguards_educ.html
Federal/ Security	*"Stop. Think. Click: Seven Practices for Safer Computing"* http://www.OnGuardOnline.gov
Federal/ Security	*NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems:* Provides guidance on developing an Information Security Plan and includes a sample plan in Appendix C. http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
Federal/ Security	*NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, Appendix A* http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
Federal/ Security	*NIST SP 800-26, Security Self-Assessment Guide For Information Technology Systems* *http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf*
Federal/ Security	*NIST SP 800-53, Recommended Security Controls for Federal Information Systems* http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf
Federal/ Security	*NIST SP 800-61, Computer Security Incident Handling Guide Special Publication* http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
Federal/ Security	*NIST SP 800-30, Risk Management Guide for Information Systems* http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
Private Industry/ Security	*Industry Standards and Best Practices* – Many private industry companies provide best practice advice on protecting information systems and safeguarding customer data. You can get more information on industry standards and best practice by researching the Internet and other resources.

6. Glossary

Adware Computer advertising software that may or may not monitor computer use to target ads.

Authorized IRS *e-file* Provider A business authorized by the IRS to participate in IRS *e-file* as an Electronic Return Originator, an Intermediate Service Provider, a Reporting Agent, a Software Developer, an Online Provider, or a Transmitter.

Confidentiality Restrictions placed on information access and disclosure, including means for protecting personal privacy and proprietary information.

Electronic Return Originator (ERO) Authorized IRS *e-file* Provider that originates the electronic submission of returns to the IRS.

Encrypt To convert plaintext to unintelligible text using a cryptographic algorithm.

Enrolled Agent A person who has earned the privilege to practice before the Service, that is, represent taxpayers, before the Internal Revenue Service.

Identity Theft Misuse of someone else's personal information to obtain new accounts or loans or commit other crimes.

Information Resources Information and related resources, such as staffing, funding, and information technology.

Information Security The process that ensures the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information System A set of information resources designated for the organization of data for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology Equipment, system, or subsystem of equipment that is used in the handling of data. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Integrity The authenticity or unimpaired condition of information; including reliability for non-repudiation of origin.

Intermediate Service Provider An Intermediate Service Provider receives tax returns from EROs (or from a taxpayer or tax exempt organization that files electronically using a personal computer, modem or the Internet, and commercial tax preparation software), processes the return information, and either forwards the information to a Transmitter, or sends the information back to the ERO (or the taxpayer or exempt organization).

Intrusion Detection The act of detecting actions that attempt to compromise the confidentiality, integrity, or availability of a resource.

IRS *e-file* The brand name of the electronic filing method established by the IRS.

Management Safeguards The security safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security.

Non-repudiation The process in which there is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity for future validation purposes.

Online Provider An Online Provider allows taxpayers to self-prepare returns by entering return data directly into commercially available software, software downloaded from an Internet site and prepared off-line, or through an online Internet site.

Operational Safeguards Security for an information system that is primarily implemented and executed by people rather than by a system.

Reporting Agent Provider that prepares and originates the electronic submission of employment tax returns for its clients. A reporting agent is an accounting service, franchiser, bank, service bureau, or other entity that complies with Revenue Procedure 2003-69, 2003-2 C. B. 403, and is authorized to perform one or more of the acts listed in Revenue Procedure 2003-69 on behalf of a taxpayer.

Risk The likelihood that the unwanted impact of an incident will be realized.

Risk Assessment The process of identifying risks and determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

Risk Management The process of managing risks through risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process includes consideration of effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

Safeguard Protective measures prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Security Controls Safeguards designed to protect the confidentiality, integrity, and availability of a system and its information.

Security Plan Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Security Requirements Requirements that are derived from laws, policies, instructions, regulations, or business (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Service Provider Any individual or business that maintains, processes, or is given access to customer information through the provisions of a service agreement with another individual or business.

Software Developer Software Developers develop software for the purposes of (a) formatting electronic return information according to publications issued by the IRS and participating states that set forth electronic return file specifications and record layouts for tax returns; and/or (b) transmitting electronic tax return information directly to the IRS.

Spyware Software installed into an information system to gather information on individuals or organizations without their knowledge.

Tax Preparer Any person who is engaged in the business of preparing or assisting in preparing tax returns.

Technical Safeguards Controls for a system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat Any circumstance or event with the potential to adversely impact operations, assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Transmitter A Transmitter will send the electronic return data directly to the IRS. EROs and Reporting Agents may apply to be Transmitters and transmit return data themselves, or they may contract with accepted Third-Party Transmitters that will transmit the data for them. A Transmitter must have software and computers that allow it to interface with the IRS.

Trojan horse A computer program used to attack a computer system by secretly allowing, among other things, unauthorized access or alteration of data or software.

User Individual or system process authorized to access an information system.

Virus A computer program used to compromise a computer system by performing functions that may be destructive. A virus may alter other programs to include a copy of itself and execute when the host program or other executable component is executed.

Vulnerability Weakness in a system through procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Worm A computer program used to compromise a computer system by impacting performance. A worm can travel from computer to computer across network connections replicating itself.

NOTE

The Electronic Tax Administration of the Internal Revenue Service prepared this guide as an outreach educational effort for all tax preparers, transmitters, and software developers. If you have any comments or suggestions for future updates, please contact:

Internal Revenue Service
SE:W:ETA:S:SP
Safeguarding Taxpayer Data Business Guide
NCFB C4-182
5000 Ellin Road
Lanham, MD 20706
.