Safeguarding Taxpayer Data

A Guide for Your Business

Contents

1. The Need to Safeguard Taxpayer Data 2

2. How to Safeguard Taxpayer Data 3

Getting Started 3

Putting Safeguards in Place 4

3. Reporting Incidents 8

4. Laws and Regulations 9

5. Standards and Best Practices 10

6. Glossary 11

1 The Need to Safeguard Taxpaye

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

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

There are a growing number of laws, regulations, standards, and best practices t cover the privacy and security of taxpayer data. This guide references those that 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 acces and data recovery.

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

2 How to Safeguard Taxpayer Data

Getting Started

If you handle taxpayer information you may be subject to the Gramm-Leach Bliley Act (GLB Federal Trade Commission (FTC) Financial Privacy and Safeguards Rules. Whether or not y the GLB Act and the FTC Rules, you could benefit from implementing the general processes a outlined in FTC information privacy and safeguards guidelines.

Financial institutions as defined by FTC include professional tax preparers, data processors, t and service providers who are significantly engaged in providing financial products or service take the following steps to protect taxpayer information. Other businesses, organizations, and handling taxpayer information should also follow these steps because they represent best pra

- Take responsibility or assign an individual or individuals to be responsible for safeguards;

- Assess the risks to taxpayer information in your office, including your operations, physical en computer systems, and employees, if applicable. Make a list of all the locations you keep taxp tion (computers, filing cabinets, bags, and boxes taxpayers may bring you);

- Write a plan of how you will safeguard taxpayer information. Put appropriate safeguards in p

- Use only service providers who have policies in place to also maintain an adequate level of protection defined by the Safeguards Rule; and

- Monitor, evaluate, and adjust your security program as your business or circumstances char

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

To safeguard taxpayer information, you must determine the appropriate security controls for y ment based on the size, complexity, nature, and scope of your activities. Security controls are ment, operational, and technical safeguards you may use to protect the confidentiality, integri availability of your customers' information. 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 information before throwing it in the trash.

For additional examples of security controls, refer to the National Institute of Standards and T (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 inform 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 information.	☐	☐	☐
Ask service providers to give you a copy of their written security policy on safeguarding information.	☐	☐	☐

FACILITIES SECURITY	ONGOING	DONE	N/A
Protect from unauthorized access and potential danger (e.g., theft, floods, and tornados) all places where taxpayer information is located.	☐	☐	
Write procedures that prevent unauthorized access and unauthorized processes.	☐	☐	
Assure that taxpayer information, including data on 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 information, including data on hardware and media.	☐	☐	
Lock doors to file rooms and/or computer rooms.	☐	☐	
Provide secure disposal of taxpayer information, 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 Rev 1, Guide for Developing Security Plans for Federal Information Systems, 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 information sign nondisclosure agreements on the use of confidential taxpayer information.	☐	☐	☐
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 information (e.g., login IDs and passwords) for those employees who are terminated or who no longer need access.	☐	☐	☐
For each employee who is terminated, conduct an exit interview and ensure the employee returns property that allows access to taxpayer information (e.g., laptops, media, keys, identification cards, and building passes).	☐	☐	☐
Train staff on Rules of Behavior for access, non-disclosure, and safeguards of taxpayer information. Provide refresher training periodically.	☐	☐	☐