Privacy and Security Rules

…at a Glance

- **The Gramm-Leach-Bliley Act: The Safeguards Rule** requires financial institutions, which include return preparers, data processors, transmitters, affiliates, service providers, and others who are paid and significantly engaged in providing financial products or services that include preparation and filing of tax returns, to ensure the security and confidentiality of customer records and information. Financial institutions must develop, implement, and maintain a written Information Security Program that contains administrative, physical, and technical safeguards that are appropriate. The Safeguards Rule is available at *http://www.ftc.gov.*

- **The Gramm-Leach-Bliley Act: The Privacy Rule** requires financial institutions, which include return preparers, data processors, transmitters, affiliates, service providers, and others who are paid and significantly engaged in providing financial products or services that include preparation and filing of tax returns, 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 Privacy Rule is available at *http://www.ftc.gov*.

- **Internal Revenue Code (IRC) § 7216** 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. IRC § 7216 is available at *http://www4.law.cornell.edu/uscode.*

- **Internal Revenue Code (IRC) § 6713** imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns. A copy of IRC § 6713 is available at *http://www4.law.cornell.edu/uscode.*

Information Security Incidents

An information security incident is an adverse event or the threat of an event that can result in an unauthorized disclosure, misuse, modification, or destruction of information.

Incidents can affect the confidentiality, integrity, and availability of taxpayer information or the ability for a taxpayer to prepare or file a return.

Types of incidents include:

- Theft of information
- Loss of information
- Natural disaster such as a flood, earthquake, or fire that destroys unrecoverable information
- Computer system/network attacks such as malicious code, or denial of service

Reporting Incidents

Who to notify in the event of an information security incident varies from one incident to another. For incidents that compromise a taxpayer's identity or their personal or financial information, refer to the Federal Trade Commission (FTC) article, "Information Compromise and the Risk of Identity Theft: Guidance for Your Business" located at *http://www.ftc.gov*. It provides guidance on when to contact local law enforcement, the FBI, the U.S. Secret Service, the U.S. Postal Inspection Service, affected businesses, and customers.

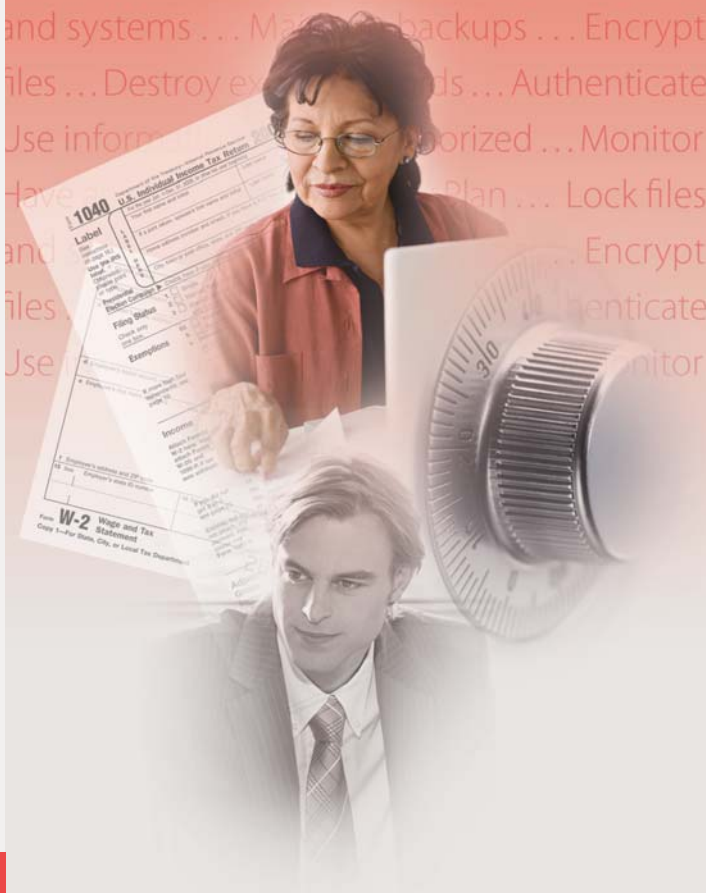
The National Institute of Standards and Technology (NIST) provides security guidelines and practices for federal agencies that nongovernmental organizations may also use. See *http://csrc.nist.gov/* for more information.

IRS Department of the Treasury Internal Revenue Service Publication 4600 (5-2007) Catalog Number 50166X
www.irs.gov

Encrypt files . . . Destroy expired records . . . Authenticate . . . Use information only as authorized . . . Monitor for breaches . . .

Safeguarding
Taxpayer Information

Quick Reference Guide for Business



Information Safeguards Shortlist

Introduction

Safeguarding taxpayer information is a top priority for the Internal Revenue Service. It is the responsibility of governments, businesses, organizations, and individuals that receive, maintain, share, transmit, or store taxpayers' personal data.

Taxpayer information is any information furnished in any form or manner (e.g. on paper, verbally, electronically, in person, over the telephone, by mail, etc.) by or on behalf of a taxpayer for preparation of their return. It includes but is not limited to a taxpayer's name, address, identification number, income, receipts, deductions, exemptions, and tax liability. IRS *e-file* and paper Return Preparers, Intermediate Service Providers, Software Developers, Electronic Return Originators, Reporting Agents, Transmitters, their Affiliates and Service Providers, and others who handle taxpayer information should understand the risk of data privacy and security breaches, and take preventative measures.

This pamphlet contains some basics on information security rules, safeguards, and incidents. Information security rules require businesses and individuals to use safeguards to protect taxpayer information from events that can result in unauthorized use, identity theft, fraud, or destruction of information. The following shortlist of information safeguards contains security measures used by governments and private companies to comply with security rules. The safeguards that businesses and individuals put into practice should be appropriate for the size, complexity, nature and scope of their business activities.

Additional guidance is available in IRS Publication 4557, *Safeguarding Taxpayer Data: A Guide for Your Business* at *www.irs.gov*

Email comments to Safeguard.data.tp@irs.gov

1 MAKE A LIST of all the locations you receive, store, or transmit taxpayer information.

- Residence, self-storage facilities, office buildings, temporary return preparation sites
- Boxes, filing cabinets, desk drawers
- Computers, optical disks, zip drives, USB removable media (thumb drives, memory sticks)

2 ASSESS THE RISK of unauthorized access, use, disclosure, modification, or destruction of the taxpayer information you handle.

- Can visitors access taxpayer information you keep?
- Can an employee with malicious intentions modify taxpayer information on a return?
- Can return preparation software you provide for customers cause an inadvertent disclosure of one taxpayer's information to another?
- Can a computer virus corrupt taxpayer returns you transmit?
- Can a flood destroy paper and electronic taxpayer records you maintain?

3 ASSESS THE IMPACT of unauthorized access, use, disclosure, modification, or destruction of taxpayer information you handle.

- Can your client become the victim of identity theft?
- Can a denial of service attack cause you to lose customers?
- Can your business incur criminal or civil penalties?

4 WRITE AND FOLLOW AN INFORMATION SECURITY PLAN that shows how you are addressing risks. There are examples of Information Security Plans on the internet.

- Describe the paper/electronic information system(s) you use to handle taxpayer information.
- Document the safeguards you need and have.
  - Locks on file cabinets and doors
  - Backups of taxpayer records
  - Background checks, information security training, and identity authentication for employees who have access to taxpayer information
  - Electronic information system passwords that meet industry standards for strong passwords
  - Encryption of taxpayer information electronically stored and during electronic transmissions
  - Firewalls, routers, or gateways to protect computer systems used for taxpayer information
  - Automatic updates of antivirus and antispyware software
  - Monitoring of computer system logs for unauthorized access
  - Authorization requirements for the removal of taxpayer information on any media
  - Requirements and the capability to securely destroy expired taxpayer information (e.g. shredders for paper and overwrite software for hard drives)
  - Security certification for computer systems used for taxpayer information

5 SPECIFY IN CONTRACTS with service providers the safeguards they must follow. Monitor how contractors handle taxpayer information.

6 TEST, MONITOR, AND REVISE your Information Security Plan on a periodic basis.

- Can you recover records from backup files and systems if primary records are destroyed?
- Do you prohibit and avoid leaving taxpayer information unsecured on desks or photocopiers, in mailboxes, vehicles, trash cans, or rooms in the office or at home?
- Are your employees following information security procedures?
- Did your computer system pass vulnerability testing?
- Are you using shredders when discarding paper taxpayer records?
- Are your contractor service providers following an acceptable Information Security Plan?

7 PUT IN PLACE ADDITIONAL SAFEGUARDS as needed.

8 PROVIDE PRIVACY NOTICES and practices to your customers, if required by the Federal Trade Commission Privacy Rule.

9 FOLLOW YOUR FEDERAL, STATE, AND LOCAL LAWS AND REGULATIONS.

Increase customer confidence and trust . . . Protect your credibility . . . Identify risk of breaches . . . Have an Information Security Plan . . . Lock files & systems . . . Maintain backups . . .