Basic Tax Exempt Bond Training – Phase I

Student Guide

This material was designed specifically for training purposes only. Under no circumstances should the contents be used or cited as authority for setting or sustaining a technical position.

IRS

Department of the Treasury
Internal Revenue Service

publish.no.irs.gov

Trng 11204
Catalog Number
8/2008

The IRS Mission

Provide America's taxpayers top quality service by helping them understand and meet their tax responsibilities and by applying the tax law with integrity and fairness to all.

IRS

Department of the Treasury
Internal Revenue Service

Document 6897 (Rev. 9-98)
Catalog Number 62293V

www.irs.ustreas.gov

Penalty for Unauthorized Inspection of Tax Returns or Tax Return Information

On August 5, 1997, President Clinton signed into law the Taxpayer Browsing Protection Act. The Act adds a new section 7213A to the Internal Revenue Code (Code) that provides a criminal misdemeanor penalty for the willful, unauthorized inspection of tax return information. The penalty is a fine of up to $1,000 and/or imprisonment up to 1 year. It applies to all Federal employees, state employees, and contractors who receive Federal tax information. Upon conviction, a Federal employee is dismissed from employment.

The Act also amends section 7431 of the Code to provide an expanded cause of action for civil damages for unauthorized inspections as well as disclosures of return or return information. Damages are $1,000 or actual damages, whichever is greater.

The expanded cause of action applies to Federal employees, state employees and contractors who knowingly, or by reason of negligence, inspect or disclose returns or return information. However, no liability will arise if the inspection or disclosure results from a good faith, but erroneous, interpretation of section 6103 of the Code (current law) or which is requested by the taxpayer (new). Section 7431 is further amended to require notification of the taxpayer for unlawful inspection or disclosure. Such notification is to be made by the IRS when a person is indicted for the misdemeanor penalty.

The Act's provisions are effective for inspections or disclosures made on or after August 5, 1997.

Internal
Revenue
Service

IDRS Security

IDRS users are authorized to access only taxpayer information (accounts) to carry out their official tax administration duties. Employees, to include IDRS users, are not authorized to initiate an access to their own records, or records of: their spouse and any ex-spouse; their children; their parents; anyone living in their household; their other close relatives; friends or neighbors with whom they have close relationships; celebrities, when the information is not needed to carry out tax related duties; an individual or organization for which they or their spouse is an officer, trustee, general partner, agent, attorney, consultant, contractor, employee, or member, and any other individual or organization with which they may have a personal or outside business relationship that could raise questions about their impartiality in handling the tax matter.

When employees are working assigned cases or contacts, they can access other IRS employees' tax records. However, when the employee working the case knows the other employee, the case must be referred to management for reassignment. If in doubt, at any time, employees need to ask their managers whether an access is authorized.

Additional information regarding unauthorized access can be found in the Supplemental Guide for IRS' Awareness Briefing on Unauthorized Access - UNAX (Document 10391 (12-98)).

Department of the Treasury
Internal Revenue Service
Document 9300 (9-94)

Ten Core Ethical Principles *

Honesty
Integrity/Principled
Promise-Keeping
Loyalty
Fairness
Caring and Concern for Others
Respect for Others
Civic Duty
Pursuit of Excellence
Personal Responsibility/Accountability

The Five Principles of Public Service Ethics *

Public Interest
Objective Judgment
Accountability
Democratic Leadership
Respectability

*Used by permission of the Michael and Edna Josephson Institute of Ethics

☆ U.S. GOVERNMENT PRINTING OFFICE: 1994 - 387-111/00133

Privacy Principles

Principle 1: Protecting taxpayer privacy and safeguarding confidential taxpayer information is a public trust.

Principle 2: No information will be collected from a taxpayer that is not necessary and relevant for tax administration and other legally mandated or authorized purposes.

Principle 3: Information will be collected, to the greatest extent practicable, directly from the taxpayer to whom it relates.

Principle 4: Information about taxpayers collected from third parties will be verified to the greatest extent practicable with the taxpayers themselves before action is taken against them.

Principle 5: Personally identifiable taxpayer information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.

Principle 6: Personally identifiable taxpayer information will be disposed of at the end of the retention period required by law or regulation.

Principle 7: Taxpayer information will be kept confidential and will not be discussed, nor disclosed to, any person within or outside the IRS other than as authorized by law and in the performance of official duties.

Principle 8: Browsing, or any unauthorized access of taxpayer information by any IRS employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.

Principle 9: Requirements governing the accuracy, reliability, completeness, and timeliness of taxpayer information will be such as to ensure fair treatment of all taxpayers.

Principle 10: The privacy rights of taxpayers will be respected at all times and every taxpayer will be treated honestly, fairly, and respectfully.

Privacy Points

1. Collect the necessary information. *

No information will be collected from or about taxpayers that is not necessary and relevant for tax administration. Our approach to information gathering will rely on data, analysis, and objective measures.

2. Treat taxpayers and co-workers with honesty, integrity, and respect.

Every taxpayer will be treated honestly, fairly, and respectfully. IRS employees, whether in a taxpayer's office or home, will refrain from physical searches of a taxpayer's mailbox and unconsented browsing of a taxpayer's mail and records.

Privacy protection begins in the workplace. Sensitive employee data must be carefully protected and employees should be treated with honesty, fairness, and respect.

3. Use the information for the purpose for which it was collected. *

Personally identifiable taxpayer information will be used only for the purpose for which it was collected and will be disposed of at the end of the required retention period.

Browsing, or any unauthorized access of taxpayer records by any IRS employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.

4. Keep information confidential.

Protecting taxpayer privacy and safeguarding confidential taxpayer information is a public trust. Taxpayer data will not be disclosed to any person within or outside the IRS, other than as authorized by law and in the performance of official duties.

* Collection of information in points 1 and 3 refers to the gathering of personally identifiable data from taxpayers or third party sources.

Protecting Taxpayer Privacy

Protecting taxpayer privacy and safeguarding confidential information is a public trust.

Privacy protection is broader than just confidentiality (disclosure) and security, although it certainly includes confidentiality and security as well.

We recognize that the majority of employees do respect the privacy of taxpayers and other employees. We are asking all IRS personnel to take a careful introspective look at how they view the privacy of taxpayers, as well as the privacy of other employees. We want to emphasize that even in commonly accepted practices, often unstated, we want each manager and employee to reevaluate how they interact with the taxpayer and with each other.

There are several reasons why the IRS needs to be very concerned with the privacy of the American taxpayer.

Voluntary Compliance - Many experts from inside and outside the IRS tell us that people may not voluntarily comply with tax laws if they think their personal information is being abused.

Shareability of Data -With the increased development of integrated information systems within IRS and accelerating shared data across government, there is an increased risk of an invasion of privacy.

Renewed Interest of the Taxpayer - Taxpayers and their representatives in Congress are taking a renewed interest in taxpayer privacy rights. The Big Brother menace seems to be more real to many people now than ever before. Investigations of employees browsing taxpayer files have heightened the fears and concerns of taxpayers and the oversight committees in Congress.

Stakeholder Concept*

Any decisions made by IRS employees should be based on the Stakeholder Concept*, developed by Michael Josephson.

> *In the Stakeholder Concept*, each person or group affected by a decision holds a moral claim on the decision maker. It is a systematic way of perceiving and sorting out the various interests involved in decision making. It reinforces the obligation to make all reasonable efforts to foresee possible consequences.*

The model employs these basic steps:

- Consider all stakeholders and ethical principles using principled reasoning. Then clarify, evaluate, decide, implement, monitor, and modify, as necessary, to ensure ethical behavior.

- Ethical values trump non-ethical values; that is, ethics must prevail.

- One may sacrifice ethical values only if it is clearly necessary to do so in order to advance other ethical values to produce the greatest balance of good in the long run.

Notices and Disclaimers

The Document Locator Numbers (DLNs), Employer Identification Numbers (EINs), Social Security Numbers (SSNs), Individual Taxpayer Identification Numbers (ITINs), Preparer Tax Identification Numbers (PTINs), Credit Card Numbers, Checking Account Numbers, Phone Numbers, and Direct Deposit Routing Numbers used in this course are hypothetical. They were constructed by random selection of numbers to appear realistic and increase the effectiveness of the training. Any duplication of numbers actually assigned is purely coincidental. All other names and numbers used in this material are fictitious.
(IRM 0420.1)

The taxpayer and business names and addresses shown in this publication are fictitious. They were chosen at random from a list of names of counties in the United States.

Basic Tax Exempt Bond Training

Phase I

Table of Contents