COMMONWEALTH OF VIRGINIA
DEPARTMENT OF TAXATION

PROCEDURES FOR SAFEGUARDING FEDERAL TAX INFORMATION

Revised

December 2008

Procedures for Safeguarding Federal Tax Information

Section	Contents	Page
	Introduction	3
	Key Facts	3
I.	Employee Perspective	4
II.	Disclosure Officer	5
III.	Federal State Tax Information Coordinator	5
	▪ Federal Safeguarding Management Analyst Sr.	6
IV.	Federal State Tax Information Co-coordinators	6
	▪ Federal State Tax Information Security Analysts	7
V.	Safeguards Afforded to Federal Information	
	IRS Tape Inventory System	7
	Downloading of Federal Data	7
	Controlling and Safeguarding Combinations and Keys	8
VI.	IT Operations Services Virginia Information Technologies Agency/NG	9
VII.	Agency Users of Federal Information	
	▪ Office Audit Section	9
	▪ Criminal Investigation Unit (CIU)	10
	▪ Revenue Analysis and Planning Unit (RAP)	10
	▪ Central Office Collections	10
	▪ District Offices	10
	▪ Office of Revenue Forecasting	10
	▪ Information Technology Staff (IT)	11
	▪ Compliance Planning UNIT (CPU)	11
	▪ CGI-AMS	12
VIII.	Office Audit Section -Revenue Agent Reports (RAR) Inventory System	13
IX.	Office Audit Section - Federal Transcript Tracking System	13

Introduction

The Department of Taxation and the Internal Revenue Service have an official exchange agreement for coordination of Federal and State tax administration. This agreement allows the Department to receive many types of federal information used in various compliance programs within the Department. Under the terms of the agreement, it is the responsibility of the Department to ensure that Federal tax returns and return information are not disclosed (UNAX) to unauthorized persons or used for unauthorized purposes. UNAX is an IRS acronym for the Willful Unauthorized Access and Inspection of Taxpayer Information.

Internal Revenue Code §7213 prescribes criminal penalties for Federal and State employees and others who make illegal disclosures (UNAX) of tax information. Code of Virginia §58.1-3 supports the Internal Revenue Code, with additional criminal provisions for State employees making unauthorized disclosures (UNAX). In addition, §7431 of the Internal Revenue Code prescribes civil damages for unauthorized disclosure (UNAX). Procedures outlined in the manual are intended to provide assistance and guidance in assuring that the practices, controls, and safeguards the department employs adequately protect the confidentiality of the data the IRS provides us. By following the procedures outlined in this manual, the Department of Taxation will meet the safeguard requirements of '§6103 of the Internal Revenue Code.

In August 1997, the *Taxpayer Browsing Protection Act* was signed into law. Browsing, or unauthorized *inspection*, is the examination either willfully or negligently of confidential tax records without an assignment or work-related reason for doing so. Penalties for browsing can include a fine, imprisonment, and being sued for damages by the injured party.

The Department's primary liaison official with the Internal Revenue Service is the Disclosure Officer. The Disclosure Officer is responsible for implementing safeguard procedures and ensuring the provisions of the exchange agreement are followed. The Disclosure Officer appoints a Federal State Tax Information Coordinator who is responsible for the day-to-day administration of disclosure (UNAX) and safeguard procedures (i.e., requests, storage, handling, destruction, etc.)

Key Facts

- All unauthorized disclosures (UNAX) of federal tax information should be reported directly to the Disclosure Officer.
- Suspected browsing of federal tax information may be reported to the local Office of the Treasury Inspector General for Tax Administration at (202) 283-3000 or the Integrity Hotline at (800) 366-4484. The Disclosure Officer should also be notified to insure TAX management is aware of potential problems.
- Any request for additional employees to be authorized to access federal tax information or to request information directly from the IRS should go to the Federal State Tax Information Coordinator.
- Any questions relating to safeguard procedures for receipt, movement, storage, or destruction of federal tax information should go to the Federal State Tax Information Coordinator.
- Any request for federal transcripts, magnetic tapes containing federal information, or any other media containing federal information should go to the Federal State Tax Information Coordinator.

Section I

Employee Perspective

How is Federal Information used by the Department of Taxation?

Confidential federal tax information is used individually and collectively to ensure compliance with Virginia tax laws through assessment, location of taxpayers, collection of taxes owed, and litigation. Information is also obtained to assist Virginia citizens in the preparation of returns to promote voluntary compliance with Federal and Virginia tax laws.

How do I request Federal Information?

All requests for confidential federal tax information must be based on a job-related need to know. The Office Audit Section is responsible for coordinating requests for federal tax information on behalf of the Department of Taxation. A Federal Transcript Request form must be completed and given to your Section Transcript Coordinator (STC) who will transmit your request to Office Audit. REFER TO SECTION VIII - OFFICE AUDIT SECTION - FEDERAL TRANSCRIPT TRACKING SYSTEM. When the federal data is received from the IRS, the data will be given to your STC who will transmit the information to you.

Am I responsible for safeguarding the federal information in my possession?

Yes. The handling of Federal information must meet federal safeguarding provisions as stated in IRS Publication 1075 (Tax Information Security Guidelines) at all times. Federal information must be stored in bar-locked cabinets when not in use and at the end of each day. Under no circumstances can federal information be permanently attached to office files that are stored in Central Files or the Warehouse. Federal data cannot be faxed or released to unauthorized parties. While the federal information is in your possession, YOU are responsible for ensuring its security from unauthorized parties.

What do I do with the federal data when I no longer need it?

Return federal transcripts to your Section Transcript Coordinator who will return the data to Office Audit for destruction. Other forms of federal information should be given to your Section Manager who will account for the destruction or return the information to the Federal/State Tax Information Coordinator in the Office Audit Section for destruction. The process used by the Department of Taxation to ensure proper disposal of federal data is known as “Document Destruction”. The Department is required by the IRS to account for all federal information received and its use prior to destruction. Furthermore, the destruction of federal information must be witnessed. Bins are located throughout the Department for disposing of information as follows:

- Witness Destruction - Grey (Federal Information)
- All other Destruction - Blue (State Information)

Tax Processing Operations- Mail Services Section collects the locked bins/containers and transports the contents for destruction. Nikki Bennett the Office Manager for Mail Services, or authorized staff witnesses this process. The IRS Witnessed Destruction Bins must be locked at all times and must not be overfilled. Managers are required to monitor the bins in their areas and notify Nikki Bennett the Supervisor of the Mail Services before the bins are filled to total capacity.

Section II

Disclosure Officer

The Departments primary liaison with the Internal Revenue Service is the agency's Disclosure Officer, Don Staples, Director of Compliance Planning, Office of Customer Relations, (804) 786-1534.

The Disclosure Officer is appointed by the Tax Commissioner and is responsible for implementing safeguard procedures. The Disclosure Officer appoints a Federal/State Tax Information Coordinator to handle the daily administration of disclosure and safeguard procedures (i.e., requests, storage, handling, destruction, etc.). In addition, the Disclosure Officer appoints a Federal/State Tax Information Co-coordinator to be responsible for the development, implementation, and maintenance of safeguard procedures within the automated system.

The Disclosure Officer or the designated appointee conducts periodic safeguard inspections throughout the year in areas that receive Federal tax returns or return information. These areas include Office Audit Section, Criminal Investigation Unit (CIU), Revenue Analysis and Planning Unit (RAP), Collections Section, District Offices (including Home Based Staff), and the Office of Fiscal Research (OFR). Periodic safeguard inspections cover the following topics:

- Handling and storage of Federal tax information
- Authorized lists of employees allowed to view Federal tax information
- Assessment of security safeguards
- Separation of Federal tax information from State tax administrative files
- Security of storage space and files during non-duty hours
- Access to combination locks and keys to locked rooms
- Security considerations during instances of planned organizational changes

If an employee discovers a possible improper disclosure of federal tax information, the individual making the observation or receiving information should contact the Disclosure Officer. The Disclosure Officer will then evaluate the nature of the disclosure and report the finding to the appropriate IRS Officer.

Section III

Federal/State Tax Information Coordinator

The Federal/State Tax Information Coordinator is responsible for the administration and coordination of most of the agency safeguard functions and requirements. The coordinator serves as the primary contact for the actual receipt of federal tax information. The Coordinator is Cheryl E. Fox, Manager, Office Audit Section, Office of Customer Relations, (804) 786-2165. In addition, Arlene Tanner, Safeguarding Management Analyst Senior for Office Audit, assist the Coordinator with federal safeguarding issues. Managers utilizing and storing federal information on site are responsible for safeguarding federal information within their sections. For example, the Manager of RAP would be responsible for safeguarding printouts with federal information used within the RAP Unit and changing the lock combinations within that office. As part of the safeguard program, the Federal/State Tax Information Coordinator is responsible for the following:

- Completion of the annual Safeguard Activity Report
- Completion of the Safeguard Procedures Report
- Updating the publication and maintenance of:
  - Procedures for Safeguarding Federal Tax Information
  - Agreement between the Virginia Information Technologies Agency (VITA)/NG and the Department of Taxation
  - Implementation Agreement between IRS and Taxation
- Changing combinations and locks
- Obtaining and maintaining an updated list of authorized employees who have access to Federal tax information
- Ensuring that employee awareness programs are in place and conducted on a periodic basis; (i.e. annual federal recertification, initial and ongoing training sessions on confidentiality of federal and state tax information, etc.)
- Maintaining inventories of magnetic media containing federal information and ensure tapes are properly safeguarded and records provide proper control and accountability, including proper destruction
- Reviewing of procedures and reports governing the access and destruction
- Communicating the request, receipt, movement, and storage of federal information
- Maintaining inventories of the federal abstracts (Revenue Agent Reports) sent to the Office Audit Section and the federal transcripts requested for the Department of Taxation, including ensuring proper safeguarding of the data and accounting of destruction
- Document the need and use of Federal Tax Information
- Prepare annual enrollment agreements for receipt of federal magnetic media
- Authorize agency users as the State Principal for Transcript Delivery System and ensure documents are stored and destroyed properly.
- Authorizing all access to FTI, both physical and electronic locations.

Federal Safeguard Management Analyst Senior

(Assistant to Federal/State Tax Information Coordinator)

Safeguarding Management Analyst Senior, Arlene Tanner of Office Audit, assists the Federal/State Tax Information Coordinator with daily Safeguarding issues. The analyst completes all reports and IRS documents for Coordinator's review and also assists with responsibilities for the coordination of most of the agency safeguard functions and requirements.

Section IV

Federal/State Tax Information Co-Coordinators

The Federal/State Tax Information Co-Coordinator is responsible for the development, implementation, and maintenance of safeguard procedures within the automated system. The co-coordinator also ensures that access is limited to only users authorized while federal data resides in the system's memory. The co-coordinator serves as the primary contact between the agency and the Virginia Information Technologies Agency. Currently, the Co-coordinator for the IRMS (Integrated Revenue Management System) is Mike Garner, of Office of Technology - Information/Technology Support. The Co-coordinator for information stored in a PC database environment in the RAP Unit and Office Audit Section is Van Nguyen, of the CPU Unit.

Mike Garner, Federal/State Tax Information Co-Coordinator is responsible for updating the Access to Federal Tax Information Report. The report lists every access to FTI via IRMS, who has access and their access privileges. The report will be prepared quarterly and sent to Cheryl

Fox, the Federal/State Tax Information Officer, for distribution to TAX Supervisors.

The TAX Managers/Supervisors will be required to respond via email to Cheryl Fox. They will validate the access or submit the required form for access changes.

Federal/State Tax Information Security Analysts

The Information Technology Safeguard Analyst (Dee Birk) and the Disclosure Specialist (Betsy Marks) are the positions created within the Department to elevate the level of safeguard inspection with respect to both, Federal and State information. They are responsible for the design and development of the procedural and software solutions to maintain the security of confidential data and to detect security violations within the agency.

Betsy Marks and Dee Birk conduct periodic safeguard inspections of the offices receiving federal tax information to ensure safeguarding procedures outlined in the IRS publication 1075 are being followed. A standard questionnaire is utilized to assist in the inspection.

Section V

Safeguards Afforded to Federal Information

Handling of Magnetic Tapes and Printouts Containing Federal Data

The Federal/State Tax Information Coordinator, who is responsible for the physical custody of the tapes, receives CDs containing extracts from the Revenue Agent Reports and occasionally paper copies of RARs. The IRS mails the CDs to the agency's physical address at 3600 West Broad Street. They are forwarded unopened to the FTC. The Office Audit Section has an IRS Tape Inventory System utilizing a paradox database to track the receipt and destruction of federal media. The Office Services Assistant/Federal Transcript Coordinator updates the inventory log of media upon receipt. A copy of the transmittal sheet is kept for recordkeeping. Magnetic media cartridges are no longer physically received at Tax or VITA/NG. Older tapes are still being returned from VITA/NG to Tax/ Computer Operations, when no longer needed. The tapes are stored in a double locked cabinet providing a two-barrier protection. Only the Federal/State Tax Information Coordinator and the Safeguarding Management Analyst have keys to these cabinets. All procedures outlined in the agreement between VITA/NG and the Department of Taxation are followed. Furthermore, a segregation of physical custody and record keeping responsibilities occurs within Office Audit.

Magnetic Tapes are destroyed annually by a degaussing process, which is completed by the Federal Safeguard Management Analyst Sr. and a designated witness. The Federal Safeguard Management Analyst Senior in Office Audit then updates the log with the deleted tapes and the destruction date. An annual tape inventory is conducted and a tape inventory report is completed and submitted to the Federal/State Coordinator. Computer Operations personnel are notified to coordinate the corresponding purge of any back up tapes stored within VITA/NG.

The Electronic Data Exchange (EDX) also known as Secure Data Transfer (SDT) has replaced the manual process of receiving tape cartridges. Greg Gentry, Agency Administrative Manager within CPU, receives electronic FTI. The information required via the SDT agreement is tracked on a spreadsheet and updated by authorized personnel in CPU.

Downloading of Federal Data

Downloading of federal data to an individuals hard drive or to portable storage devices (floppy disks/disk drives) is strongly discouraged. Written approval must be obtained from Cheryl Fox, Federal/State Tax Information Coordinator.

If the federal information is downloaded to diskette or other portable media, the authorized individual will be responsible for ensuring the portable media and any related printouts are stored in locked cabinets when the data is not in use and at the end of each day.

Requests to ship Federal tax information must be made to the Federal State Tax Information Coordinator. The Coordinator will verify the need for the transporting of data before the shipment will be allowed. Instructions for safeguarding and returning the documents are included with each document shipment. The Coordinator will maintain a log of all documents sent and returned to the Department of Taxation.

Federal tax information will be clearly labeled and mailed by overnight courier in doubled sealed envelopes and marked "FEDERAL RETURN INFORMATION NOT TO BE OPENED EXCEPT BY THE ADDRESSEE". Personnel receiving the information are reminded that federal tax information cannot be duplicated and may not be improperly disclosed (UNAX).

Employees are responsible for safeguarding federal tax information in their possession. During non-work hours, federal materials are stored in locked file cabinets. When the materials are no longer needed, the information is returned to the Federal State Tax Information Coordinator by overnight courier with the language indicated above. The Coordinator will account for the destruction of the media and ensure the proper disposal or destruction thereof.

Controlling and Safeguarding Combinations and Keys

Keys and combinations to high-security work areas, container rooms, filing cabinets, where IRS tax information is maintained are restricted to authorized personnel. Combinations and keys are given only to those employees with an identifiable need to know and a need to have access to locked filing cabinets. The Federal/State Tax Information Coordinator maintains documentation regarding personnel possessing safe combinations or keys. A record showing the key control number, locked area, key type, name, issue date, and return date if applicable is maintained for each key access.

The Supervisor of Computer Operations, Pat Moran is responsible for safeguarding the federal data contained in the temporary holding cabinet located in that section. The cabinet must have a double- barrier lock protection. The supervisor maintains a log indicating changes to the combination lock that is used on this cabinet.

The Section Managers are required to notify Cheryl Fox, Federal/State Tax Information Coordinator immediately of any changes to staff, locks or combinations that are needed or if access has been compromised. The locks will be maintained and distributed by Cheryl Fox or the Safeguard Analyst Arlene Tanner only. All keys are logged into a database showing the employees having possession of keys and reconciled annually. In addition, annually a confirmation will be sent to all employees in possession of keys and validating any changes needed acknowledging ownership.

Section VI

IT Operation Services

Automated Data Processing System (IRMS)

The Department's automated data processing (ADP) system is a batch processing system named IRMS. The ADP system is used to compare federal and state information in order to identify discrepancies for audit by various Compliance units.

Data is stored on magnetic tapes in sequential access files and processed off-site, at the Virginia Information Technologies Agency data center with remote job entry at the Taxation Department. Authorized contractors are used in connection with the processing, storage, transmission, and destruction of Federal tax information stored on electronic media.

The Department security system continues to be maintained and exceeds the C2 level of protection required by the IRS. The operating security features of the system meet each of the four requirements outlined in IRS Publication 1075.

Control over processing at Virginia Information Technologies Agency (VITA)/NG

The Department of Taxation and the Virginia Information Technologies Agency (VITA)/NG, have implemented a Memorandum of Agreement for processing Federal tax information. This agreement establishes the safeguard procedures, which must be followed by VITA/NG employees when processing Federal tax information at the computer center.

Designated agency personnel transport federal magnetic media (tapes) to and from the VITA/NG computer service center and Tax's computer Operations Section. The tapes are released only to designated VITA/NG personnel. A list of designated personnel is maintained in the Departments Operation Service area. A Senior Systems Operations employee monitors the movement and storage of all Federal tax tapes. VITA/NG also maintains a list of all employees who have access to these tapes.

Federal tax tapes are stored in a secured tape storage cabinet with restricted access based on job function. Janitorial services in this area are performed only in the presence of VITA/NG Systems Operation personnel.

The VITA/NG Office of Internal Audit reviews procedures implemented at VITA/NG to safeguard Federal data and conducts safeguard inspections at the processing site. A written audit report is issued annually.

Section VII

Agency Users of Federal Tax Information

The Office of Customer Relations - Compliance is the principle user of federal tax information from the IRS. Other areas within the Department also utilize information obtained from the IRS as authorized.

Office Audit Section

The Office Audit Section is one of the main users of federal tax information. The section utilizes federal information on tapes for the individual non-filer programs, the individual federal compare program, and the CP2000 program. These programs are computerized and information is maintained in Tax operating systems (IRMS and STARS). All older magnetic media tapes are stored in a double-locked cabinet providing a two-barrier protection maintained by the Federal/State Tax Information Coordinator as required by the IRS.

The Office Audit Section also receives IRS audit abstracts (Revenue Agent Reports) for use in Office Audit compliance programs, and federal transcripts on behalf of the Tax Department. Inventories, including records of destruction, are maintained in the section utilizing a Paradox database system. The documents are stored in bar-locked cabinets until they are assigned to selected staff. At the end of the day, all files containing federal information are returned to the bar-locked cabinets in drawers assigned to each worker. When a file is completed, the IRS document is filed in the federal room bar-locked cabinets. Refer to Office Audit Section - Revenue

Agent Report (RAR) Inventory System and Office Audit Section - Federal Transcript Tracking System for additional information.

Criminal Investigation Unit (CIU)

The manager logs Federal tax information received. All requested federal tax information is maintained in a bar-locked file cabinet. While cases are ongoing, CIU investigators may request federal information either orally or in writing from the Unit Manager. Any requests for federal tax information on taxpayers with out-of-state addresses are routed to Federal/State Tax Information Coordinator for approval. The manager or Federal Safeguard Analyst through agency mail service in a double sealed envelope marked “FEDERAL RETURN INFORMATION NOT TO BE OPENED EXCEPT BY THE ADDRESSEE” mails any information requested by a CIU field investigator.

Revenue Analysis and Planning Unit (RAP)

The RAP Unit utilizes information from federal magnetic and electronic tapes, disks, federal returns, and from transcripts. Electronic Transmissions of FTI data are received by Greg Gentry, Agency Administrative Manager. FTI such as Transcripts in RAP are stored in file cabinets with lock bars when not in use. Only personnel with a need to know are authorized to handle such information.

Collections Unit

Collections periodically search the IRMF tape for bank lien sources on cases in various states in CACSG (Computer Assisted Collections System for Government). This matching process is repeated until a valid lien source is found or all sources are exhausted.

District Offices

Requests for Federal tax information from district offices are made to the designated Section Transcript Coordinator. The Coordinator maintains a log of all documents sent to and returned from district offices.

When confidential IRS data is mailed to field personnel the employee receiving the material is informed of the shipment in advance and shipments are documented on transmittal forms and monitored to ensure that each shipment is properly and timely received and acknowledged.

Personnel in the district offices as well as home based staff receive Federal tax information in a double sealed envelope addressed to the employee, by overnight courier. The envelope will be clearly marked "*FEDERAL RETURN INFORMATION NOT TO BE OPENED EXCEPT BY THE ADDRESSEE"*. District office personnel and home based staff are reminded that federal tax information cannot be duplicated and should not be shared with anyone except those who have a need to know. While in their possession, district office employees and field agents are responsible for safeguarding federal tax information as outlined in the provision of IRS publication 1075. During non-work hours, the Federal tax information is sealed and stored in a locked file cabinet. When federal tax information is no longer needed, the information is returned to the Office Audit Transcript Coordinator by overnight courier with the language indicated above.

Office of Revenue Forecasting

The Federal/State Tax Information Coordinator receives a magnetic tape containing a sample of Federal returns filed by taxpayers with Virginia addresses from the IRS Statistics of Income Tape Library D:R:S:P. The tape is logged and handled according to procedures for all other federal tapes.

No data concerning specifically identified taxpayers will be released to anyone outside of the Department of Taxation. No statistical tabulation will be released with cells containing data from fewer than three returns. Access to the merged data set is restricted to economists within the Office of Revenue Forecasting. Access to the merged data set, either in computer tape or printed form, by other State non-Tax personnel will not be allowed. When not being used, any printouts not deemed presentable to the public (i.e., listings with cells containing fewer than three returns) will be stored within the Office of Revenue Forecasting. The tabulations are statistical and do not identify specific taxpayers or confidential federal information.

Information Technology Staff (IT) and Compliance Planning Unit (CPU)

Information Technology Staff (IT Staff) and Compliance Planning Unit Staff (CPU) are subject to the same safeguard requirements and penalties for failure to safeguard federal data that apply to all agency employees.

The main users of Federal Data in IT and CPU are Operations staff, Database Administrators, Application Developers, Quality Control and IT Security personnel, however, all IT and CPU Staff must be familiar with how to safeguard Federal Tax Data. IT and CPU Staff use Federal Tax Data to test functionality in various systems such as:

- Audit Compliance Repository
- Advantage Revenue
- Siebel
- Audit Case Management
- CACSG – Computer Assisted Collections System for Government

They test compliance programs in these systems by performing audit matches, checking filing dates, non-filing occurrences, FTI comparison, under reported income on the Virginia returns, and the availability of various schedules.

When using Federal Tax Data, IT Staff must remove Federal Tax identifiers such as Social security numbers, names, and addresses. If Federal Tax Data identifiers cannot be removed, written justification must be provided and formal approval obtained from OT Management in order to use data in this manner.

Some IT Staff have access to this data on an on-going basis as long as the need is justified. The access is verified quarterly with the Application Developer's manager by the Federal Safeguard Coordinator.

Federal Tax Data is stored on the Virginia Information Technology Agency (VITA)/NG mainframe, and on windows based servers on the TAX Network. This Federal Tax Data is stored as read-only access. IT Staff, and specifically Application Developers, are allowed to copy files from here to approved alternate secured, shared directories on the mainframe and windows based servers for further analysis or importing into the various systems shown above. Copying these files to locations (potentially unsecured) other that the following locations pose disclosure risks:

- Mainframe – Windows Based Servers designated in quarterly FTI report.
- TAX.RAP – S:\RAP or S:\taxdata\C2 or M:\OOCOA

Please contact the IT Risk Management group for further guidance on approved storage locations to store Federal Tax Data.

Access to Federal Tax Data on the server is tracked through the use of Audit Logs. These logs capture what data has been accessed, and the date/time for each occurrence. In addition, access to the electronic Federal Tax Data is limited to the specific time period that a person needs access. In addition, random scans are performed on PCs to ensure that no Federal Tax Data is stored inappropriately.

- When copying Federal Tax Data to approved alternate, secured directories, IT Staff should rename the files to something that does not easily identify them as containing Federal Tax Data.

- Once IT Staff no longer need access to Federal Data, they must immediately notify their supervisor so access can be removed. The supervisor if needed can easily reinstate access.

Here are some key points for IT Staff to bear in mind when safeguarding Federal Tax Data.

- Do NOT leave your screen unattended with Federal Data on it; logoff PC, use a password protected screensaver if you need to leave your PC unattended, or lock your computer every time you leave your desk. If you do not, there is the potential for an unauthorized disclosure (UNAX) for which you will be held accountable.

- Do NOT share your password with anyone.

- Do NOT copy Federal Tax Data to your PC or removable media of any kind.

- Do ensure that you need access to Federal Tax Data. If you do not, contact your supervisor or manager immediately to have access removed.

- Do NOT provide a file of federal data or even a screenshot of Federal Tax Data to another IT Staff member (including subordinates) who has not been authorized for access to Federal Tax Data. Doing so constitutes disclosure (UNAX).

- Remember, there is no such thing as test data that contains federal data or was built from federal data unless all identifiers have been removed – otherwise it is Federal Data pure and simple and must be protected in that manner.

- Application Developers are the only group within Office of Technology that is allowed to print Federal Tax Data during the course of Systems testing. If YOU DO – ensure that the information is SHREDDED or placed in an orange tag bin for destruction when the information is no longer needed. Printed federal tax data must be properly secured when not in use and at the close of each business day until the information is properly destroyed.

- Use of Internal email is OK for IT Staff ONLY IF identifiers are first removed and they enable Lotus Notes Digital Signatures and Encryption. (Search the Lotus Notes Help for how to do this or contact the Help Desk.) Use of external email to send Federal Tax Data is prohibited.

- If IT staff need to use Internal Mail for Federal Tax data, they should use an “orange “Hand Deliver sticker, and place the information in a double sealed envelope marked:
  “Federal Return Information – Not to be opened except by addressee”

- When mail is delivered by authorized personnel it should be handed to the designated person on the “Hand Deliver” sticker only.

CGI-AMS - Federal Data Access Requests

All CGI-AMS staff working with Federal Tax Information receives safeguarding and disclosure (UNAX) training before access is granted. The Federal Safeguard Coordinator maintains a log of CGI-AMS staff trained in Federal Safeguarding procedures.

Section VIII

Office Audit Section - Revenue Agent Reports (RAR) Inventory System

The Office Audit Section receives paper federal audit reports (RARS) and EOAD CDs from the IRS Philadelphia Service Center and/or the IRS Richmond District Office for use in Office Audit compliance programs. Audits are received for individual income tax, corporate income tax, and estate tax. All mail received from the IRS remains unopened. Authorized designated personnel in the mailroom record receipt in the tracking system the mail is forwarded to the Federal/State Tax Information Coordinator (FTC). The FTC or designated representative records receipt in the mail tracking system and verifies the information on the transmittal sheet with the actual inventory received. This individual signs the transmittal form and returns the form to the IRS as verification of receipt. The federal documents are given to the Office Audit Clerical Supervisor who is responsible for stamping the audits with the date of receipt. All audits are marked "State Copy" in red by the IRS and all are stored in bar-locked cabinets when not in use.

The Office Audit Clerical Supervisor logs the receipt of each audit or CD in the Office Audit RAR Inventory System. This system, which was implemented in August 1997, utilizes a Paradox database and is password protected. The data is stored on a network drive, under a subdirectory accessible only to select Office Audit employees. Each audit record is assigned a unique control number in addition to the following information: social security number or EIN, tax period, info type, tax type, name, address, request section, reason for request, assignment (team), date mailed from IRS, date received by Tax Department, destroy date, destroy method, and any pertinent comments. All audits are placed in bar-locked cabinets to be worked by Office Audit Auditors and Tax Examiner Seniors. They are carefully safeguarded until destruction. The Federal/State Information Coordinator is responsible for documenting and ensuring the proper destruction of federal RAR audit information.

Section IX

Office Audit Section - Federal Transcript Tracking System

Effective calendar year 2005, the Office Audit Section began using the IRS Transcript Delivery System (TDS) to retrieve federal transcripts direct from the IRS website. TDS automates the validation, processing and delivery of taxpayer information to the authorized third party user, thus requiring less intervention from IRS personnel. TDS has decreased the turnaround time to facilitate completion of audit activity at the state level. On behalf of the Tax Department, the Office Audit Section is the central area for requesting, receiving, tracking and destroying federal transcripts and related data such as account transcript return transcripts, statement of account, hard copies of returns, and microfiche. The Federal/State Tax Information Coordinator is responsible for overseeing these functions.

Accordingly, a Federal Transcript Tracking System was implemented utilizing a Paradox database, which is password protected. The information is stored on a network drive, under a subdirectory accessible only to selected Office Audit employees. The Office Audit Section receives requests from the designated Section Transcript Coordinators (STC) of the Agency as listed:

Criminal Investigation Unit (CIU) -Rhonda McGarvey
Collections Section including Office Audit -Sarah Comstock
Customer Services -Jeremy Armstrong
Revenue Analysis and Planning (RAP) -Eric Armstrong
District Offices -James Mason
Appeals and Rulings -David Mason
Customer Satisfaction - Clare Dunn

Each area Section Transcript Coordinator (STC) is responsible for coordinating the individual requests and submitting the IRS Transcript Request Forms to the Office Audit Section Transcript Coordinator (OASTC), Sarah Comstock.

The OASTC enters the request information into the IRS website and is able to retrieve the federal transcript within 1 to 2 business days. Each request is assigned a unique control number in the Federal Transcript Tracking System. The OASTC enters the following information for each case: SSN or EIN, tax type, tax period, form type, taxpayer name, taxpayer address, and reason code for the request which identifies the requesting section, requester, request date, date from IRS, date sent to STC, estimated destruction date, actual destruction date, destruction method and IRS tracking number.

Each Section Transcript Coordinator (STC) that requested federal information receives a report "Summary of IRS Return Requests - Section Transcript Coordinator" detailing the following: date given to coordinator, control numbers, taxpayers names, SSN(s) or EIN(s), tax type, tax period, requestor section, request date, received date, total number of requests, and signature for approval. Each STC must physically pick up the federal transcripts with the exception of the District Offices and home-based staff. District Offices and home-based staff receive Federal Information through the mail using a double sealed envelope.

Sections receiving federal transcripts are required to safeguard the federal information in locked cabinets when the data is not in use and at the end of each day. The Office Audit Section maintains a bar-locked cabinet for the Revenue Analysis and Planning Section (RAP). All federal transcripts stored in the Office Audit Section meet federal safeguarding provisions as outlined in IRS Publication 1075.

All Federal transcripts are to be returned to the Office Audit Section for destruction when no longer needed. If a destroy date is not indicated, the transcript may be destroyed 60 days from the date the document was received by the Tax Department. Effective immediately, the OASTC will distribute a list of all outstanding transcripts annually that are over 1 year old with no destruction date documented in transcript database to each STC. This list will be used to verify that the requestor still has the federal tax information in their possession. Each STC will respond with an update on the pending destruction date.

Safeguarding Organizational Structure

Who's Who in Safeguarding
Quick Reference

Don Staples Agency Disclosure Officer
Cheryl Fox Federal Safeguarding Coordinator
Mike Garner Federal/State Tax Information Co-coordinator
Betsy Marks Federal Disclosure Specialist
Dee Birk Information Technology Safeguard Analyst
Van Nguyen Federal/State Tax Information Co-coordinator for PC Database
Arlene Tanner Federal Safeguarding Management Analyst
Sarah Comstock Federal Transcript Coordinator