540 Control

# Publication 1075

## Tax Information Security Guidelines For Federal, State and Local Agencies

*Safeguards for Protecting Federal Tax Returns and Return Information*


IRS

**TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND LOCAL AGENCIES OMB No. 1545-0962**

Paperwork Reduction Act Notice

The Internal Revenue Service (IRS) asks for the information in the Safeguard Procedures Report and the Safeguard Activity Report to carry out the requirements of the Internal Revenue Code (IRC) Section 6103(p).

You are not required to provide the information requested on a form that is subject to the Paperwork Reduction Act unless the form displays a valid Office of Management and Budget (OMB) control number. Books or records relating to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, Federal Tax Returns and return information are confidential, as required by IRC Section 6103.

The information is used by the IRS to ensure that agencies, bodies, and commissions are maintaining appropriate safeguards to protect the confidentiality of Federal Tax Information (FTI). Your response is mandatory.

The time needed to provide this information will vary depending on individual circumstances. The estimated average time is 40 hours.

If you have any comments concerning the accuracy of these time estimates or suggestions for making this publication simpler, we would be happy to hear from you. You can write to us at:

Tax Products Coordinating Committee
Internal Revenue Service, SE:W:CAR:MP:T:T:SP
1111 Constitution Avenue, NW, IR-6406
Washington, DC. 20224

*Preface*

This publication revises and supersedes Publication 1075 (October 2007).

This page left intentionally blank.

## HIGHLIGHTS FOR 2010

### COMPUTER SECURITY CONTROLS

This document provides updated requirements using the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, revision 3. In addition, this document contains updated controls to include testing of the computer security controls, and additional physical and personnel security controls based on NIST Special Publication (SP) 800-53, for the moderate impact level.

Note: While the Safeguards Office has responsibility to ensure the protection of Federal Tax Information, it is the responsibility of the organization to build in effective security controls into their own Information Technology (IT) infrastructures to ensure that this information is protected at all points where Federal Tax Information (FTI) is received, processed, stored and/or maintained. It will not be the intent of IRS to monitor each control identified but to provide these to the organization, identifying those controls required for the protection of moderate risk systems within the federal government.

### SUBMITTING REPORTS AND CORRESPONDENCE

Correspondence, reports, attachments, requests for technical assistance, requests for current templates, etc., should be emailed to the Safeguard mailbox: SafeguardReports@irs.gov.

Safeguards recommends that all required reports be submitted using IRS approved encryption methods.

### INTERNET ACCESS

Agencies can access Publication 1075 on the Internet by going to http://www.irs.gov and searching for "Publication 1075."

The IRS.gov website contains guidance, job aids, helpful tools and frequently asked questions to assist agencies in meeting safeguard requirements. URL: http://www.irs.gov/businesses/small/article/0,,id=177651,00.html

### REPORTING UNAUTHORIZED DISCLOSURES

Unauthorized inspection or disclosure of Federal tax information, including breeches and security incidents, must be reported immediately to the appropriate Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards using the procedures outlined in section 10.0

### APPEAL PROCESS RELATED TO POSSIBLE SUSPENSION AND/OR TERMINATION OF TAX DATA

Title 26 U. S. Code Section 6103(p)(4) requires external agencies and other authorized recipients of Federal tax return and return information (FTI) to establish procedures to ensure the adequate protection of the FTI they receive. That provision of the Code also authorizes the Internal Revenue Service (IRS) to take actions, including suspending or terminating FTI disclosures to any external agencies and other authorized recipients, if there is misuse and/or inadequate safeguards in place to protect the confidentiality of the information. The Federal tax regulation 26 CFR 301.6103(p)(7)-1 establishes a consistent appeal process for all authorized recipients of FTI. See Exhibit 3.

This page left intentionally blank.

TABLE OF CONTENTS

This page left intentionally blank.

### *1.1 General*

The Internal Revenue Service (IRS) is acutely aware that in fostering our system of taxation, the public must maintain a high degree of confidence that the personal and financial information furnished to us is protected against unauthorized use, inspection, or disclosure.

Therefore, we must administer the disclosure provisions of the Internal Revenue Code (IRC) according to the spirit and intent of these laws, ever mindful of this public trust. The IRC makes the confidential relationship between the taxpayer and the IRS quite clear. It also stresses the importance of this relationship by making it a crime to violate this confidence. IRC Section 7213 prescribes criminal penalties for Federal and State employees and others who make illegal disclosures of federal tax returns and return information (FTI), which is a felony offense. Additionally, IRC Section 7213A makes the unauthorized inspection of FTI a misdemeanor punishable by fines, imprisonment, or both. And finally, IRC Section 7431 prescribes civil damages for unauthorized inspection or disclosure and upon conviction, the notification to the taxpayer that an unauthorized inspection or disclosure has occurred.

The sanctions of the IRC are designed to protect the privacy of taxpayers.

Similarly, the IRS recognizes the importance of cooperating to the fullest extent permitted by law with other federal, state, and local authorities in their administration and enforcement of laws. The concerns of citizens and Congress regarding individual rights to privacy make it important that we continuously assess our disclosure practices and the safeguards we use to protect the confidential information entrusted to us.

*The Internal Revenue Service is acutely aware that in fostering our system of taxation the public must have and maintain a high degree of confidence that the personal and financial information furnished to us is protected against unauthorized use, inspection, or disclosure.*

Those agencies or agents that receive FTI directly from either the IRS or from secondary sources (e.g., Health and Human Services, Federal entitlement and lending agencies) must have adequate programs in place to protect the data received. Furthermore, as agencies look more to "contracting out" certain services, it becomes equally important that those with whom contracts exist protect that information from unauthorized use, access, and disclosure.

### *1.2 Overview of Publication 1075*

This publication provides guidance in ensuring that the policies, practices, controls, and safeguards employed by recipient agencies or agents and contractors adequately protect the confidentiality of the information they receive from the IRS.

Enterprise security policies shall address the purpose, scope, responsibilities, and management commitment to implement all applicable security controls. This document contains the managerial, operational, and technical security controls that should be implemented as a condition of receipt of FTI.

The guidelines outlined herein apply to all FTI, no matter the amount or the media in which it is recorded. FTI in

electronic form must be afforded the same levels of protection given to paper documents or any other media containing FTI. Security policies and procedures – systemic, procedural or manual – should minimize circumvention.

A mutual interest exists in our responsibility to ensure that FTI is disclosed only to authorized persons and used only as authorized by statute or regulation. The IRS is confident of your diligence in this area and believes that Publication 1075 will be helpful.

Conforming to these guidelines meets the safeguard requirements of IRC Section 6103(p)(4) and makes our joint efforts beneficial.

Requirements throughout Publication 1075 apply to all organizational segments of an agency receiving FTI. It is the agency's responsibility to ensure all functions within their agency, including consolidated data centers and contractors (where allowed by federal statute), with access to FTI understand and implement the Publication 1075 requirements.

This publication provides the preliminary steps to consider before submitting a request to process FTI, provides requirements to properly safeguard information, explains what to expect from the IRS once the information has been disclosed, and suggests miscellaneous topics that may be helpful in setting up your program. Exhibits 1 through 14 are provided for additional guidance.

The IRS Office of Safeguards is responsible for all interpretations of safeguarding requirements. Publication 1075 requirements may be supplemented or modified between editions of Publication 1075 via guidance issued by the Office of Safeguards and posted on their IRS.gov web site.

The IRS.gov website contains guidance, job aids, helpful tools and frequently asked questions to assist agencies in meeting safeguard requirements. URL: http://www.irs.gov/businesses/small/article/0,,id=177651,00.html

Publication 1075 can be accessed through the Internet at www.irs.gov.

### *2.1 General*

Section 6103 of the IRC is a confidentiality statute and generally prohibits the disclosure of FTI (see Exhibit 1, *Confidentiality and Disclosure of Returns and Return Information, for general rule and definitions*). However, exceptions to the general rule authorize disclosure of FTI to certain federal, state, and local agencies. Generally, these disclosures are made by the IRS in response to written requests signed by the head of the requesting agency or delegate. FTI so disclosed may be used by the receiving agency solely for the purpose described in the exception authorizing the disclosure. The statutes providing authorization to disclose FTI contain specific conditions that may require different procedures in maintaining and using the information. These conditions are outlined under specific sections in this publication.

As a condition of receiving FTI, the receiving agency must show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information. Safeguards must be designed to prevent unauthorized access and use. Besides written requests, the IRS may require formal agreements that specify, among other things, how the information will be protected. An agency must ensure its safeguards will be ready for immediate implementation upon receipt of FTI. Copies of the initial and subsequent requests for data and of any formal agreement must be retained by the agency a minimum of five years as a part of its record keeping system. Agencies should always maintain the latest Safeguard Procedures Report (SPR) on file. The initial request must be followed up by submitting an SPR. It must be submitted to the IRS at least 45 days before the scheduled or requested receipt of FTI (see section 7.0, *Reporting Requirements*).

The SPR should include the processing and safeguard procedures for all FTI received, and it should distinguish between agency programs and functional organizations using FTI.

Multiple organizations, divisions or programs within one agency using FTI may be consolidated into a single report for that agency, with permission of the Office of Safeguards. Entering into any agreement for disclosure to agents or contractors of an agency requires advance notice to the Office of Safeguards (see section 11.3)

*An agency must ensure its safeguards will be ready for immediate implementation upon receipt of FTI. Enterprise security policies shall address the purpose, scope, responsibilities, and management commitment to implement associated controls.*

**Note:** Agencies should use care in outlining their safeguard program. Reports that lack clarity or sufficient information will be returned to the submitting agency.

### *2.2 Need and Use*

Any agency that receives FTI for an authorized use may not use that information in any manner or for any purpose not consistent with that authorized use. If an agency needs FTI for a different authorized use under a different provision of IRC Section 6103, a separate request under that provision is necessary. An unauthorized secondary use is specifically prohibited and may result in discontinuation of disclosures to the agency and imposition of civil and/or criminal penalties on the responsible officials.

The Office of Safeguards conducts "need and use" reviews as part of the safeguard review and always considers if the agency's

use is in conformance with the governing provisions allowing the disclosure of FTI.

### *2.3 Obtaining FTI*

The IRS has established a Secure Data Transfer (SDT) program to provide encrypted electronic transmission of FTI between the IRS and trading partners. This method secures the data during transmission and has replaced the distribution of magnetic tape cartridges by the IRS.

### *2.4 State Tax Agency Limitations*

FTI may be obtained by state tax agencies only to the extent the information is needed for, and is reasonably expected to be used for, state tax administration. An agency's records should include some account of the result of its use of FTI (e.g., disposition of closed cases and summary of revenues generated) or include reasons why the information was not used. If any agency continually receives FTI that for any reason it is unable to use, it should contact the IRS official liaison and discuss the need to stop disclosures so they no longer receive this FTI. In conformance with IRC 6103(d), IRS will disclose FTI only to the extent that a state taxing agency satisfactorily establishes that the requested information can reasonably be expected to be used for tax administration purposes.

State tax agencies using FTI to conduct statistical analysis, tax modeling or revenue projections must notify the IRS by submitting a signed *Need and Use Justification for Use of Federal Tax Information for Tax Modeling, Revenue Estimation or Other Statistical Purposes* and following the established guidelines.

Annually, the agency will provide updated information regarding their modeling activities which include FTI in their Safeguard Activity Report. In the annual SAR, the agency must describe:

- any use of FTI that is in addition to what was described in the original Need and Use Justification
- any new, previously unreported internal tax administration compilations that include FTI
- Changes to the listing of authorized employees (Attachment B to the Need and Use Justification)

If the agency intends to use a contractor for conducting statistical analysis, tax modeling or revenue projections, they must submit a 45-day notification (see section 11.3) prior to contractor access to the FTI. The agency's Safeguard Procedures Report should detail the use of FTI for this purpose. In addition, the agency must submit a separate statement detailing the methodology used and data to be used by the contractor. The Office of Safeguards and Statistics of Income functions will review the information provided to confirm that appropriate safeguarding protocols are in place and that the modeling methodology to be used to remove taxpayer identifying information, is appropriate.

### *2.5 Coordinating Safeguards within an Agency*

Because of the diverse purposes that authorized disclosures may be made to an agency and the division of responsibilities among different components of an agency, FTI may be received and used by several quasi-independent units within the agency's organizational structure. Where there is such a dispersal of FTI, the agency should centralize safeguarding responsibilities to the greatest extent practical and establish and maintain uniform safeguard standards consistent with IRS guidelines. The official(s) assigned these responsibilities should hold a position high enough in the agency's organizational structure to ensure compliance with the agency safeguard standards and procedures. The selected official(s) should also be responsible for ensuring that internal inspections are

conducted, for submitting required safeguard reports to the IRS, for properly reporting any data breach incidents, and for any necessary liaison with the IRS.

### *2.6 Safeguard Reviews*

A safeguard review is an on-site evaluation of the use of FTI and the measures employed by the receiving agency to protect the data. This includes FTI received from the IRS, the Social Security Administration (SSA), or other agencies. Safeguard reviews are conducted to determine the adequacy of safeguards as opposed to evaluating an agency's programs. IRS regularly conducts on-site reviews of agency safeguards. Several factors will be considered when determining the need for and the frequency of reviews. Reviews are conducted by the Office of Safeguards, within the Office of Communication, Liaison, and Disclosure Office (CLD:S).

### *2.7 Conducting the Review*

*A safeguard review is an evaluation of the use of FTI received from the IRS, the Social Security Administration, or other agencies and the measures employed by the receiving agency to protect that data.*

The IRS initiates the review by verbal communication with an agency point of contact. The preliminary discussion will be followed by a formal engagement letter to the agency head, giving official notification of the planned safeguard review.

The engagement letter outlines what the review will encompass; for example, it will include a list of records to be reviewed (e.g., training manuals, flowcharts, awareness program documentation and organizational charts relating to the processing of FTI), the scope and purpose of the review, a list of the specific areas to be reviewed, and agency personnel to be interviewed.

Reviews cover the six requirements of IRC Section 6103(p)(4): Record Keeping, Secure Storage, Restricting Access, Other Safeguards (covering employee awareness and internal inspections), Reporting Requirements, and Disposal. Computer Security and Need and Use are a part of Restricting Access but appear in the report under their own headings. The six requirements are covered in depth in this publication.

The on-site review officially begins at the opening conference where procedures and parameters will be communicated. Observing actual operations is a required step in the review process. Agency files may be spot-checked to determine if they contain FTI. The actual review is followed by a closing conference when the agency is informed of preliminary findings identified during the evaluation. An interim Safeguard Review Report (SRR) will be issued to document the on-site review findings.

The agency must respond to the interim SRR by submitting a Corrective Action Plan (CAP), detailing their planned actions to resolve the identified findings. Once the agency's response to the interim SRR is received, a final SRR will be issued.

The agency's response to the interim SRR includes the submission of the initial Corrective Action Plan (CAP). The CAP must be updated and submitted to the Office of Safeguards twice a year until all review findings are accepted and closed by the Office of Safeguards.

The CAP must include a brief explanation of actions already taken or planned to resolve the finding. For all outstanding findings, the agency must detail planned actions and associated milestones for resolution.

All findings should be addressed in a timely fashion. The Office of Safeguards will identify deadlines for resolution based upon the risk associated with each finding. Outstanding issues should be resolved and addressed in the next reporting cycle of the Corrective Action Plan (CAP), Safeguard

Activity Report (SAR), or, if necessary, the Safeguard Procedures Report (SPR) (see section 7.0).

**Guide 1 – Safeguard Review Cycle**

**Preliminary Discussions**
**Engagement Letter**
**Opening Conference**
**On-site Evaluation**
**Closing Conference (with Preliminary Findings)**
**Interim Report**
**Agency Response (Initial Corrective Action Plan (CAP))**
**Final Report**
**CAP Submissions Until All Findings Resolved**

### *3.1 General*

Federal, State, and local agencies, bodies, commissions, and agents authorized under IRC Section 6103 to receive FTI are required by IRC Section 6103(p)(4)(A) to establish a permanent system of standardized records of requests made by or to them for disclosure of FTI (see Exhibit 3, *Sec 6103(p)(4) Safeguards*). This record keeping should include internal requests among agency employees as well as requests outside of the agency. The records are to be maintained for five years or the applicable records control schedule must be followed, whichever is longer.

### *3.2 Electronic Files*

Authorized employees of the recipient agency must be responsible for electronic media from receipt through destruction. Inventory records must be maintained for purposes of control and accountability. Any media containing FTI or any file resulting from the processing will be recorded in a log that identifies:

- date received
- control number and/or file name & contents
- recipient
- number of records, if available
- movement
- if disposed of, the date and method of disposition.

Such a log will permit all media (including those used only for backup) containing FTI to be readily identified and controlled.

Responsible officials must ensure that electronic media containing FTI removed from the storage area is properly recorded on charge-out records. Semi-annual inventories of removable media must be conducted. The agency must account for any missing electronic media, document search efforts taken and notify the appropriate authorities as directed in section 10.0 of the loss.

### *3.3 Non-electronic Files*

A listing of all documents received from the IRS must be identified by:

- taxpayer name
- tax year(s)
- type of information (e.g., revenue agent reports, Form 1040, work papers)
- the reason for the request
- date requested
- date received
- exact location of the FTI
- who has had access to the data and
- if disposed of, the date and method of disposition.

*The agency must account for any missing electronic media, document search efforts taken and notify the appropriate authorities as directed in section 10.0 of the loss.*

If the authority to make further disclosures is present (e.g., agents/contractors), information disclosed outside the agency must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Agencies transmitting FTI from one mainframe computer to another, as in the case of the SSA sending FTI to state human services agencies and in instances where the auditors extract FTI for child support agencies, need only identify the bulk records transmitted. This identification will contain the approximate number of taxpayer records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.

### *3.4 Converted Media*

Conversion of FTI from paper to electronic media (scanning) or from electronic media to paper (print screens or printed reports) also requires tracking from creation to destruction of the converted FTI. All converted FTI should be tracked on logs containing the data elements detailed in sections 3.2 and 3.3 above, depending upon the current form of the FTI. Paper to electronic FTI logs shall reflect the data elements in section 3.2 and electronic media to paper FTI logs shall reflect the data elements in section 3.3.

### *3.5 Record Keeping of Disclosures to State Auditors*

When disclosures are made by a state tax agency to state auditors, these requirements pertain only in instances where the auditors utilize FTI for further scrutiny and inclusion in their work papers. In instances where auditors read large volumes of records containing FTI, whether in paper or electronic format, the state tax agency need only identify bulk records examined. This identification will contain the approximate number of taxpayer records, the date of inspection, a description of the records, and the name of the individual(s) making the inspection.

Disclosure of FTI to state auditors by child support enforcement and human services agencies is statutorily prohibited if the state auditors are not employed by the state. If the state auditors are contractors instead of state employees, the disclosure restrictions pertaining to contractors or agents apply. Whenever possible, FTI in case files should be removed prior to access by the auditors.

### *4.1 General*

Security may be provided for a document, an item, or an area in a number of ways. These include, but are not limited to, locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic security systems, fences, identification systems, and control measures. How the required security is provided depends on the facility, the function of the activity, how the activity is organized, and what equipment is available. Proper planning and organization will enhance the security while balancing the costs.

The IRS has categorized federal tax and privacy information as moderate risk. Guide 2 – Secure Storage, Physical Security – Minimum Protection Standards, within this document, should be used as an aid in determining the method of safeguarding federal tax information. These controls are intended to protect the systems that contain FTI. It is not the intent of the IRS to mandate requirements to those systems and/or areas that are not processing FTI.

### *4.2 Minimum Protection Standards (MPS)*

The Minimum Protection Standards (MPS) establish a uniform method of physically protecting data and systems that require safeguarding. This method contains minimum standards that will be applied on a case-by-case basis. Since local factors may require additional security measures, management must analyze local circumstances to determine space, container, and other physical security needs at individual facilities. The MPS have been designed to provide management with a basic framework of minimum security requirements.

The objective of these standards is to prevent unauthorized access to FTI. MPS requires two barriers to access FTI under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Locked means an area or container that has a lock with controlled access to the keys or combinations. A security container is a lockable metal container with a resistance to forced penetration, with a security lock with controlled access to keys or combinations. (See section 4.3.4 for secured perimeter/interior.) The two barriers provide an additional layer of protection to deter, delay, or detect surreptitious entry. Protected information must be containerized in areas where other than authorized employees may have access after hours.

Using a common situation as an example, often an agency desires or requires that security personnel or custodial service workers or landlords for non-government owned facilities have access to locked buildings and rooms. This may be permitted as long as there is a second barrier to prevent access to FTI. A security guard, custodial services worker or landlord may have access to a locked building or a locked room if FTI is in a locked container. If FTI is in a locked room, but not in a locked container, the guard, janitor or landlord may have a key to the building but not the room.

During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear picture identification badges or credentials. The badge must be clearly displayed, preferably worn above the waist.

Additional controls have been integrated into this document that map to guidance received from the National Institute of Standards & Technology (NIST). These are identified in Exhibit 4, NIST Moderate Risk Controls for Federal Information Systems. Through this document, the exhibit will simply be referenced as Exhibit 4.

Policies and procedures shall be developed, documented, and disseminated, as necessary, to facilitate implementing physical and environmental protection controls. (Exhibit 4 PE-1).