

5101:9-9-25.1 County agency federal tax information safeguarding procedures.

(A) This supplemental rule provides general guidance to county agencies on the safeguarding of federal tax information (FTI), with the exception of child support enforcement agencies, which are required to comply with the requirements of rule 5101:12-1-20.2 of the Administrative Code. Individual program offices may, at their discretion, establish additional rules and/or additional training programs. County agencies should consult their respective program office for additional information regarding the safeguarding of FTI.

(B) Required employee awareness training:

Each county agency must provide disclosure awareness training to employees and contractors in accordance with guidelines set forth in internal revenue service (IRS) publication 1075, "Tax Information Security Guidelines for Federal, State and Local Agencies." Employees and contractors must maintain their authorization to access FTI through annual training and recertification. Prior to granting an agency employee or contractor access to FTI, each employee or contractor must certify his or her understanding of the IRS's and the agency's security policy and procedures for safeguarding IRS information. Employees must be advised of the provisions of sections 7431, 7213, and 7213A of the Internal Revenue Code regarding the "Sanctions for Unauthorized Disclosure" and the "Civil Damages for Unauthorized Disclosure." The disclosure awareness training records must be maintained for a minimum of five years or in accordance with the agency's applicable records retention schedule, whichever is longer.

(C) Proper record keeping of FTI:

County agencies must keep records detailing internal requests for FTI by agency employees as well as requests received from outside of the agency, except for child support enforcement agencies, which are required to follow rule 5101:12-1-20.2 of the Administrative Code.

A tracking log must be used to record all movement, storage, and destruction of both electronic and non-electronic FTI received by the agency from the IRS. The data elements of the tracking log shall comply with the guidelines set forth in IRS publication 1075 and those provided by the applicable ODJFS program office. FTI must not be recorded on any tracking log. The logs must be maintained for a minimum of five years or in accordance with the agency's applicable records retention schedule, whichever is longer.

(D) Secure storage and handling of FTI:

(1) FTI must be handled in such a manner that it does not become misplaced or available to unauthorized staff. When not in use, FTI must be secured via the required two barrier minimum pursuant to the "Minimum Protection

Standards (MPS)" section of IRS publication 1075. Refer to table 2 in section 4.2 of IRS publication 1075 for further guidance.

- (2) Minimum protection standards establish a uniform method of physically protecting data and systems as well as non-electronic forms of FTI. Local factors may require additional security measures, therefore, local county management must analyze local circumstances to determine location, 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. Examples of two barrier minimum under the concept of MPS are outlined in IRS publication 1075.
- (3) FTI should not be filed in areas used by employees not authorized to have access to FTI such as areas used for breaks, food preparation or any similar facilities. FTI files should not be maintained in areas that allow clients access. However, when this is not practical, caution must be exercised by the agency pursuant to the "Minimum Protection Standards (MPS)" section of IRS publication 1075. Refer to table 2 in section 4.2 of IRS publication 1075 for further guidance.

(E) Restricting access to FTI:

Access to file storage areas that contain FTI must be limited to the absolute minimum number of employees necessary. The following measures should be followed to adequately restrict access to the file storage areas containing FTI:

- (1) Except where the state program office maintains records on access and training, a current list of employees who are authorized to have access to FTI shall be maintained by the county agency.
- (2) Warning signs must be posted to identify restricted access areas and to give notice of the potential consequences for unauthorized disclosure or inspection of FTI.
- (3) Cleaning, building inspections or maintenance of secured areas containing FTI, must be performed in the presence of an employee authorized to access FTI. An exception to this rule is during non-duty hours, when cleaning, inspection or maintenance personnel need access to locked buildings or rooms. This may be permitted as long as there is a second barrier to prevent access to FTI. Access may be granted to a locked building or a locked room if FTI is in a locked security container. If FTI is in a locked room but not a locked security container then access may be granted to the building but not the room.
- (4) Each agency shall control physical access to areas where systems or files containing FTI are housed. The agency shall issue authorization credentials,

including badges, identification cards, or smart cards pursuant to section 4.3.2 of IRS publication 1075.

- (5) Access to file areas that contain FTI must be restricted to agency employees who have an established security profile that identifies the class-level and role-based rights that necessitate authorizing the employee to have such access.
- (6) The location and physical layout of the file storage area should be such that unnecessary traffic is avoided.
- (7) A visitor sign in/sign out log must be maintained and must be inspected at least monthly by agency security personnel. The data elements contained on the log must meet the guidelines outlined in IRS publication 1075.
- (8) Keys to the files must be issued only to agency employees authorized to enter the secured area.
- (9) If possible, security staff should be agency employees. Only authorized employees, or escorted individuals supervised by authorized employees, may have access to areas where FTI is located during working and nonworking hours.
- (10) All records containing FTI, either open or closed, must be safeguarded pursuant to IRS publication 1075. FTI should not be commingled within any information system or within any physical files and documents. When commingling of agency documentation data and FTI is unavoidable, FTI must be labeled pursuant to IRS publication 1075, and access must be restricted to only authorized personnel.

(F) Proper disposal of FTI:

- (1) Users of FTI are required by the Internal Revenue Code to take certain actions after using FTI, to protect its confidentiality. When FTI is no longer useful, agency officials and employees must either return the information, including any copies made, to the office from which it was originally obtained or destroy the FTI.
- (2) An agency electing to return IRS information must use a receipt process and ensure that confidentiality is protected at all times during transport.
- (3) FTI (non-electronic) furnished to any authorized agency employee or user and any paper material generated therefrom, such as copies, photo impressions, computer printouts, notes, and work papers, must be destroyed pursuant to IRS publication 1075 directives.
- (4) FTI (electronic) stored in electronic format (e.g., hard drives, tapes, CDs, flash

media, etc.) must be destroyed and/or disposed of pursuant to IRS publication 1075 directives. Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing (media sanitization).

- (5) For county agencies, programs and records where contractors are permitted to be used, any destruction, sanitization, and/or disposal of FTI by a contractor must be witnessed by an agency official or employee. FTI destroyed or sanitized, pursuant to sections 8.0 to 8.4 of IRS publication 1075, is no longer considered FTI and can be disposed of in any manner the agency deems appropriate.

(G) Computer security controls:

If any local agency office stores FTI within a county owned information system, they must:

- (1) Ensure the required agreements with ODJFS and the IRS have been established pursuant to IRS publication 1075.
- (2) Ensure the local agency office's required policies, procedures, and information system meet the minimum computer system security controls detailed in IRS publication 1075.

Replaces: Part of 5101:9-9-25
Effective: 05/01/2016

CERTIFIED ELECTRONICALLY

Certification

03/24/2016

Date

Promulgated Under: 111.15
Statutory Authority: 5101.02
Rule Amplifies: 329.04
Prior Effective Dates: 5/1/93, 9/27/93, 6/26/95, 2/15/96, 11/1/96, 10/4/02, 5/23/03