# Ohio Administrative Code

## Rule 5101:12-1-22 Safeguarding of information from the internal revenue service.

Effective: November 1, 2022

(A) This rule describes the procedures a child support enforcement agency (CSEA) is required to follow in order to safeguard information received from the internal revenue service (IRS). The procedures for safeguarding federal tax information (FTI) are based upon the tax information security guidelines described in IRS publication 1075 (rev. 11/2021). IRS Publication 1075 is available at www.irs.gov. The safeguarding requirements of this rule apply to any paper, electronic, or imaged record.

(B) Failure to comply with the safeguarding requirements of this rule shall result in the revocation of access to the support enforcement tracking system (SETS) or any other computer application that contains information from the IRS.

(C) For purposes of this rule and its supplemental rules, FTI is defined as federal tax return information other than information provided by the taxpayer, including but not limited to:

(1) Address information obtained from the IRS;

(2) Social security numbers obtained from the IRS;

(3) Federal tax filing status; or

(4) Identification of the payment source as an IRS tax refund offset collection.

(D) Each CSEA shall complete and submit to the office of child support (OCS) within the Ohio department of job and family services (ODJFS) a JFS 07072, "Safeguarding of Internal Revenue Service, Ohio Department of Taxation, Federal Parent Locator Service, and Unemployment Compensation Information" (effective or revised effective date as identified in rule 5101:12-1-99 of the Administrative Code) no later than the last day of April each year. The JFS 07072 must be signed and dated by the director or administrator of the CSEA.

(E) In accordance with rule 5101:9-9-26 of the Administrative Code, each CSEA will develop a written procedure requiring all: final candidates, as defined in rule 5101:9-9-26 of the Administrative Code, current employees, prospective contractors or sub-contractors and, current contractors and sub-contractors who are or will be granted access to FTI to submit to a background investigation that is favorably adjudicated and is in accordance with the IRS publication 1075. The written procedure is to be made available to OCS and/or the IRS upon request.

(F) The CSEA shall notify OCS at least sixty days prior to re-disclosing FTI to a contractor so that OCS may notify the IRS office of safeguards at least forty-five days prior to the re-disclosure.

(G) The CSEA shall notify OCS at least sixty days prior to re-disclosing FTI to a sub-contractor so that OCS may notify the IRS office of safeguards and obtain written approval at least forty-five days prior to the re-disclosure.

(H) The CSEA shall prior to re-disclosing FTI to a contractor or sub-contractor:

(1) Establish privacy roles and responsibilities for contractors and service providers;

(2) Include privacy requirements in contracts and other acquisition-related documents;

(3) Share FTI externally only for authorized purposes and in a manner compatible with those purposes;

(4) Enter into a contract, service level agreement, memorandum of understanding, memorandum of agreement, letter of intent, computer matching agreement, or similar agreement, with third parties that specifically describes the FTI covered and specifically enumerates the purposes for which the FTI may be used;

(5) Monitor, audit, and train CSEA staff on the authorized uses and sharing of FTI with third parties and on the consequences of unauthorized use or sharing of FTI; and

(6) Evaluate any proposed new instances of sharing FTI with third parties to assess whether they are

authorized and whether additional or new public notice is required.

(I) For each individual with access to FTI that is an employee of: the CSEA; a contractor of the CSEA; or a sub-contractor to provide goods or services on behalf of a contractor of the CSEA, the CSEA shall ensure that:

(1) A background investigation is completed in accordance with rule 5101:9-9-26 of the Administrative Code;

(2) FTI safeguarding training is completed upon employment or re-employment and on an annual basis thereafter. The FTI safeguarding training shall include, but is not limited to:

(a) Disclosure awareness training;

(b) Security awareness training;

(c) Role-based training;

(d) Contingency training; and

(e) Incident response training.

(3) Each individual certifies his or her understanding of policies and procedures for safeguarding FTI by completing the FTI safeguarding training and a JFS 07014, "Tax Information Safeguarding Authorization Agreement" (effective or revised effective date as identified in rule 5101:12-1-99 of the Administrative Code).

(a) FTI safeguarding training and a JFS 07014 must be completed upon employment or re-employment and on an annual basis thereafter.

(i) An individual who has been granted access to SETS in accordance with paragraph (F) of rule 5101:12-1-15 of the Administrative Code has met this requirement.

(ii) Any other individual who has access to FTI must complete the FTI safeguarding training and a JFS 07014.

(b) The initial certification and recertification will be maintained by OCS and made available to the IRS upon request. These records are to be retained for a minimum of five years in accordance with requirements under IRS publication 1075.

(4) A permanent FTI tracking system is utilized. FTI may be tracked using any of the following methods:

(a) The FTI tracking database provided by OCS;

(b) The JFS 07019, "Federal Tax Information Item Tracking Log" (effective or revised effective date as identified in rule 5101:12-1-99 of the Administrative Code); or

(c) An alternative FTI tracking database, provided that:

(i) The database contains all of the same data elements as the JFS 07019; and

(ii) The CSEA submits the database to OCS for approval and OCS approves the database.

(5) A permanent system of standardized records is established and maintained with regard to requests made for information from the IRS that includes:

(a) The reason for the request;

(b) The date the request is made;

(c) The date FTI is received; and

(d) The name of the employee(s) having access to the information.

(6) FTI is stored during non-duty hours in accordance with the secure storage and minimum

protection standards described in IRS publication 1075;

(7) Access to file keys and safe combinations is limited to employees responsible for safeguarding FTI and a maximum of two alternates who are permitted access to the FTI;

(8) FTI is limited to those individuals who are authorized to inspect and use the information. Limiting access to FTI must meet the IRS publication 1075 standards by:

(a) Designating restricted areas;

(b) Creating an authorized access list; and

(c) Developing physical access authorizations.

(9) Commingling standards described in IRS publication 1075 are followed. FTI may be maintained either separately from a file or within a file. When FTI is maintained within a file, the outside jacket of the file shall have a label stating that the file contains FTI;

(10) Mail received containing FTI is properly labeled as described in paragraph (I)(11)(a) of this rule and is not opened before delivery to the CSEA employee, contractor, or sub-contractor responsible for safeguarding the information;

(11) Computer stations are safeguarded in accordance with standards described in IRS publication 1075. Computer stations may be safeguarded by:

(a) Restricting access to only authorized staff;

(b) Utilizing password protections;

(c) Utilizing screen savers; and

(d) Logging out of the system.

(12) Correspondence containing FTI is properly transmitted according to the following standards:

(a) When sending the correspondence by ordinary mail, the agency shall send the correspondence in a double-sealed envelope with a label on the inner envelope that alerts the recipient that the mail contains FTI;

(b) When sending the correspondence by electronic mail, the agency will only send the electronic message to a recipient within the ODJFS email system, and:

(i) Alert the recipient in the text of the electronic message that the attachment contains FTI; and

(ii) Send the correspondence as an attachment to the electronic message that is encrypted and is password protected; and

(iii) Send the password to access the attachment in a separate electronic message.

(c) When sending the correspondence by facsimile (i.e., fax), the agency shall:

(i) Include a cover sheet that alerts the fax recipient that the correspondence contains FTI and indicates the name of the intended fax recipient;

(ii) Verify that the intended fax recipient is an authorized person; and

(iii) Verify that the intended fax recipient will be present at the fax machine to receive the correspondence at the time the CSEA sends it.

(13) FTI is only destroyed in accordance with the destruction methods described in IRS publication 1075 when FTI is no longer needed by the agency and that the destruction is tracked as described in paragraph (I)(4) of this rule.