IRS Preparations

Child Support requires newly hired staff to complete the security review prior to access to any system that is provided. Annual reviews are done every July for child support workers. Workers must complete all security training and sign the required forms.

- Workers must watch the "Protecting Federal Tax Information" along with the "Safeguards Security Awareness Training" video.
- IRS Publication 1075 Exhibit 4, Sanctions for Unauthorized Disclosure and Exhibit 5, Civil Damages for Unauthorized Disclosure must be reviewed. Exhibits are in SharePoint, Security Folder, FPLS/FTI/IRS -Documents.
- A link to the IRS Protecting FTI Pocket Guide is in SharePoint. This is a quick reference guide that will provide information to staff with questions concerning FTI.

All staff must complete training videos/documents listed on the Initial/Annual Requirements Certification form. The documents should be returned to the supervisor.

- Initial/Annual Requirements Certification – the revised form now includes the new video and training.
- OCSS Agreement to Safeguard Confidential Information

The following documents are completed kept on file for 5 years per the IRS requirements:

- FPLS/IRS Security Training Exercise
- DES Acknowledgment of Confidentiality of Information
- SSA Data Memorandum of Understanding
- SSA Security Training Form
- Copy of the OCSS Agreement to Safeguard Confidential Information
- Copy of the Initial/Annual Requirements Certification

The link to the IRS Publication 1075 is also located in SharePoint. This is a great tool for any questions you may have regarding protecting IRS data.

Please remember:

1. **Please know** in case someone from IRS may ask you a question. Make sure you have watched your videos on SharePoint. Pay attention, make sure you read everything and have a good understanding when completing your exercises and security forms.
2. **Please know:** that all visitors must sign in and their badges must always be visible (including the IRS when they visit). Also, all child support staff should have their badges

on and visible always. Make sure you are using the visitors log from SharePoint that the IRS recommends we use.

3. **Please know**: It is very important to never leave your desk without doing Control+ Alt +Delete to lock your screen. Make sure to practice the clean desk policy during the IRS visit.
4. **Please know**: federal tax information should not be printed, but if you do – never ever have this information left out on your desk. There is a tax sensitive destruction log that should be kept for any FTI that you might print, must be labeled, and tracked from printing to destruction. FTI print must be kept according to the Pub 1075 2 (two) barrier requirements.
5. **Please Know**: Penalties:
    a. Unauthorized disclosure can result in fines up to $5,000.00 or 5 years in jail or both.
    b. $1,000 for each act of unauthorized inspection or disclosure of a return or return information to the plaintiff- Civil Damages or imprisonment of not more than 1 year or both.

6. **Please Know**: Your access badge should not be given to anyone. No one should come in behind you without swiping their badge or being let in by the receptionist to sign in and get a badge.
7. **Please Know**: FTI should not be scanned, emailed, or faxed. If it is, it must be encrypted, the person on the other end ready to receive it immediately and label, log and protect it appropriately.
8. **Please Know:** Our work area should be clean during the IRS visit.
9. **Please Know**: Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, the individual making the observation must report this to your manager or security officer by submitting a **Privacy and Security Office-Incident Reporting Form at https://security.ncdhhs.gov/ .**(see attached form).

    Contact the Office of IRS Safeguards immediately, but no later than 24 hours after identification of a possible issue involving FTI by email to Safeguards mailbox: safeguardreports@irs.gov

    In addition to contacting the Office of IRS Safeguards, local offices also must make these reports to the CSS Security Officer at CSS.Security@dhhs.nc.gov . CSS Central Office and

Customer Service Center reports should be made to the CSS Security Officer, in addition to contacting the Office of IRS Safeguards.

The agency must notify the Office of Safeguards by email to Safeguards mailbox, **safeguardreports@irs.gov**. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to:

- Name of agency and agency Point of Contact for resolving data incident with contact information.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- How the incident was discovered
- Description of the incident and the data involved, including specific data elements, if known
- Potential number of FTI records involved; if unknown, provide a range if possible
- Address where the incident occurred.
- IT involved (e.g., laptop, server, mainframe)

Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email. Do not include any FTI in the data Incident report.
Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information must be provided to the Office of Safeguards as soon as it is available.

10. **Please Know:** If an address is returned from FPLS with the source of IRS, the Responsible caseworkers should:

- Delete the "POTN" address record with the source code "FPLS"
- Create a "POTN" address record for the NCP with the source code "OTHR" (Other); and then,
- Generate and send a Postmaster Verification Request (DSS-4466).

- In preparation of an IRS review/audit, your county should review the following:

    - Visitor Log – a visitor log with the required elements from Pub 1075, 2.B.3.1 must be used. A sample log is available in SharePoint. The visitor log must be closed out at the end of each month and reviewed by management.
    - Authorized Access List (AAL): See Section 2.B.3.2 of IRS Pub 1075 for requirements. The AAL for employees must be updated at least annually or when employee access changes.
    - AAL – Vendors and Non-Agency Personnel – See Pub 1075 2.B.3.2 Must be updated monthly.

- Keys and Combinations - all containers, rooms, buildings, and facilities containing FTI must be locked when not in use.
- Access Control Systems (e.g., badge readers, smart cards, and biometrics – must maintain audit records with successful and failed access attempts to areas containing FTI. Agency personnel must review access control logs monthly. The access control log must contain:
  - Owner of the access control device requesting access
  - Successful/failure of request
  - Data and time of request
- FTI should rarely be printed. If printed, FTI must be entered on the FPLS/IRS Tracking/Destruction log. All movement must be tracked until destruction. FTI document must be labeled as FTI, file folder labeled, and protected by 2 barriers per the IRS Pub 1075 guidelines.
- Email/Fax/Multifactor Device Policy – staff should be familiar with the policy found in the OLM, Chapter B, Topic 2, Section F
- Disposal – Shredding must meet the IRS requirements -cross cut shredders which produce particles that are 1mm x5mm in size. See 2.F.3 of IRS Pub 1075 for more info.
- Security/confidential training forms – All staff with access to FTI must complete training and sign the form at point of hire and annually thereafter. Security forms should be kept on file for at least 5 years. The IRS may ask to see these at the onsite visit!
- FTI Improper Disclosure -all staff should know how, when, and where to report improper disclosure of FTI. The IRS reviewer may randomly select a worker and ask if they know what to do. Staff should review info in OLM, Chapter B, Topic 2, Section F.
- Computer Security – the IRS will use an automated tool to scan the workstations that are used to access FTI. Your local IT staff should become familiar with the requirements based on the IRS Pub 1075 and the State Information Security manual.
- File records – it is best to purge all case records of FTI if possible! If files do contain FTI, they must be labeled, locked, and recorded on the tracking/destruction log. The IRS may select files to review.
- FTI should not be scanned in records.

Printing Federal Tax Information -

Because pertinent FTI is stored in ACTS and general notes are recorded in ACTS (which replaces paper documentation), CSS workers MUST NOT print FTI.

If FTI is inadvertently printed or FTI that has been printed previously is discovered and cannot be destroyed, the following requirements MUST be followed:

* Any document that contains FTI must be labeled with a Notice Label 129 (unless it is already labeled), and any file folder that contains documents with FTI must be labeled with a Notice Label 29A. These labels notify the recipients that the document(s) and/or file folder(s) must be safeguarded.

* All printed FTI that is retained in the office (including ACTS screen prints, documents, reports, and/or notes containing FTI) must be protected by a two-barrier standard (EX: stored in a locked desk or cabinet that is located in a locked facility). When no longer needed, FTI must be destroyed by shredding.

* If case files are stored off-site, the files should be reviewed, and all federal tax-related material should be removed and stored within a two-barrier environment until the retention period expires. This separately stored FTI should be destroyed according to the agency's retention/destruction policy.
(Chapter B Topic 02 Section F)

Transmitting Federal Tax Information -

Transmitting Federal Tax Information – Transmitting FTI by email, fax, or printer is not recommended. If it is necessary, the following rules must be applied.

Email:

FTI must not be transmitted outside of the agency by email, either in the body of a message or as an attachment. When sending FTI through agency internal email system:

- Ensure that the message is encrypted.
- Ensure that recipients' addresses are correct.
- Always log off the computer when away from the area.
- Ensure that the email is properly labeled (ex: email subject contains “FTI” to alert the recipient to the need for confidentiality precautions.
- Ensure the message of the FPLS/IRS Sensitive Information Tracking and Destruction Log

(Chapter B, Topic 2, Section F)

Fax Policy

Transmitting Federal Tax Information – Transmitting FTI by email, fax, or printer is not recommended. If it is necessary, the following rules must be applied.

Facsimile (FAX) – To protect security of the data:

- Place fax machines in a secure area.
- Always have trusted staff at both the sending and receiving machines.
- Always include a cover sheet that contains notice of the sensitive nature of the data and instructions to an unintended recipient on the notice to the sender and destruction of the data.
- Maintain a record of any lists or preset numbers of frequent recipients of FTI.

Multifunction Devices – If FTI is transmitted via multiple-function equipment, these rules must be followed:

- FTI must be encrypted while in transit to/from the device.
- FTI must not be emailed or faxed from the device.
- FTI must not be stored on the device.
- If FTI is scanned into the device, the user must be identified by a unique password.

(Chapter B, Topic 2, Section F)

Scan policy.
Including a list of documents, you scan that may contain FTI.

No documents containing FTI are scanned.

Transmitting Federal Tax Information – Transmitting FTI by email, fax, or printer is not recommended. If it is necessary, the following rules must be applied.

Multifunction Devices – If FTI is transmitted via multiple-function equipment, these rules must be followed:

- FTI must be encrypted while in transit to/from the device.
- FTI must not be emailed or faxed from the device.
- FTI must not be stored on the device.
- If FTI is scanned into the device, the user must be identified by a unique password.

(Chapter B, Topic 2, Section F)

Chapter B02F6

Printing FPLS Information -

CSS workers should print any information that contains confidential data ONLY when necessary. Any printed material, including ACTS or State Services Portal (SSP) screen prints, reports, or other documents that contain FPLS information must be labeled to identify its confidential nature and be maintained in a locked container when not in use.

Disclosure of IRS Information to Case Participants -

Because federal tax information (FTI) about one individual is confidential, personal information about a participant that is received from the IRS (such as address, wage source/data, SSN, or other FTI) cannot be shared with another participant. However, the IRS does allow the release of limited information regarding a tax refund offset (intercept) to a custodial parent (CP - coded "CLI") in an IV-D case.

After receiving an offset payment, CSS can share the following information with the CP:

* The date of receipt.

* The amount of the payment.

* The source of the payment (IRS).

* The fact that the payment could be made for up to six (6) months.

CSS must not disclose a specific reason for the hold but should state only that offset payments are held because they might be subject to adjustment.

Although the payment histories that CSS provides to CPs and the Notice of Payments To CP (DSS-4516) document do not include a payment source, CSS can inform the CP that CSS received the payment as a tax refund intercept. The Notice of Collections To The NCP (DSS-4520) includes the payment amount, but it no longer includes the payment source due to restrictions on FTI being transmitted through the mail or
courier/messenger services.

CSS caseworkers must ensure that only the appropriate information and documents are provided to each participant and that the IRS nondisclosure rules are followed during any discussion of payment information with CPs.
(Chapter B, Topic 02, Section F)

All employees with access to FTI must submit to a mandatory FTI background investigation that consists of FBI fingerprinting, criminal record check and verification of citizenship. Background investigations are completed every five (5) years for all CSS employees. The complete CSS policy on background checks is located on the CSS SharePoint Site: https://ncconnect.sharepoint.com/sites/nccss/ . After accessing this web site, select "Forms and Documents" on the Quick Launch bar, then click on the "Supervisory Forms and Documents" page link. The "Background Checks for Potential Employees, Employees, and Contractors Access to Federal Tax Information" document is located under the "CSS Background Checks - Internal Document Links" heading. For more information, select the term: CSS SharePoint Web Site .
(Chapter B Topic 02 Section F)