	INDIANA DEPARTMENT OF CHILD SERVICES TITLE IV-D POLICY MANUAL	
	Chapter 18: Confidentiality and Security	**Effective Date: 10/31/2022**
	Section 1: Introduction to Confidentiality and Security	**Version: 1** **Revision Date: 10/31/2022**

BACKGROUND

The Indiana Title IV-D child support program is comprised of the Child Support Bureau (CSB), Title IV-D Prosecutor's Offices, and Clerks of Court. These offices are collectively referred to as the Title IV-D program. CSB and its county partners are committed to safeguarding confidential information, including Federal Tax Information (FTI) and Personal Identifiable Information (PII), pursuant to federal and State regulations.

DEFINITIONS

While this Section does not contain an all-encompassing list of terms and definitions, these are the key terms that are essential in understanding the Title IV-D program's security policies and procedures. Additional terms may be defined in other pertinent policy and procedure documents.

1. **"Confidential information"** is any information relating to a specific person including, but not limited to, the person's Social Security number, address, employment information, and financial information.[1] It includes, but is not limited to, FTI and/or PII provided by the Internal Revenue Service (IRS), Social Security Administration (SSA), and Office of Child Support Enforcement (OCSE). The Title IV-D program is required to protect from unauthorized disclosure all confidential information regardless of the source.

2. **"Data"** is a representation of facts, concepts, information, or instruction suitable for communication, processing or interpretation by people or information systems.[2] Data within the Title IV-D program may be generally categorized into one of the following categories:
    a. Public Access Data: Data that is openly available to all custodial parties (CPs), non-custodial parents (NCPs), and the general public;
    b. Internal General Data: Data used for CSB administration activities and not for external distribution unless otherwise authorized;
    c. Internal Protected Data: Data that is only available to staff with the required access in order to perform their assigned duties; or
    d. Internal Restricted Data: Data that is of a sensitive and confidential nature and is restricted from general distribution. Special authorization must be approved before access or limited access is granted. FTI and PII fall under this category. Internal restricted data that is transmitted within the statewide child support system shall be encrypted to protect its confidentiality and integrity from

[1] 45 C.F.R. § 303.21(a)(1)
[2] Publication 1075, Glossary and Key Terms

unauthorized disclosure and modification.[3] Internal restricted data that has reached its destination after its transmission within the statewide child support system shall also be encrypted to protect its confidentiality and integrity from unauthorized disclosure and modification.[4]

3. **"Federal Tax Information (FTI)"** consists of federal tax returns and/or federal tax return information.[5] FTI is any return or return information received from the IRS or an IRS secondary source, such as SSA, OCSE, Bureau of Fiscal Services (BFS), or the Centers for Medicare and Medicaid Services (CMS).[6] Any information derived from FTI is also considered FTI.[7] With respect to the statewide child support system, FTI is anything showing TX (payment type) associated with any payments, adjustment, joint return status, and locate response data (such as name, address, Social Security number, annual wage information, and self-employment indicator) from the FCR and Federal Offset Program where the locate agency code is IRS, IRS/AWR, or LTXF.

4. **"Need to know basis"** or **"least privilege"** means that a person must have access to only enough information to carry out their official duties.[8]

5. **"Personal Identifiable Information (PII)"** is information that would identify a specific person. PII means an individual's first and last name or first initial and last name and at least one (1) of the following:
    a. Social Security number;
    b. Driver's license number or identification card number; or
    c. Account number, credit card number, debit card number, security code, access code, or password of an individual's financial account.[9]

    This term does not include the last four (4) digits of an individual's Social Security number or any information that is lawfully made publicly available from records of a federal or local agency.[10]

6. **"Return information"** means any information provided in relation to the federal tax return, including, but not limited to the taxpayer's identity, income, deductions, exemptions, credits, tax liability, tax withheld, tax payments; and whether the taxpayer's return was, is being, or will be examined.[11]

POLICY

1. Location of Required Security Policies and Procedures

    As part of receiving confidential information from the IRS, SSA, and OCSE, CSB, and by extension the Title IV-D program, is required to have certain security policies and procedures in place. This Title IV-D Policy Manual contains security policies applicable

[3] Publication 1075, Section 4.18 SC-8
[4] Publication 1075. Section 4.18 SC-12
[5] Publication 1075, Key Definitions
[6] Publication 1075, Key Definitions
[7] Publication 1075, Key Definitions
[8] Publication 1075, Glossary and Key Terms
[9] IC 4-1-11-3(a)
[10] IC 4-1-11-3(b)
[11] 26 U.S.C. § 6103(b)(2)(A)

to the regular course of child support business. Additional required security policies and procedures may be found in one or more of the following locations:

a. Indiana Department of Technology (IOT) policy and procedure documents;
b. Department of Child Services (DCS) IT policy and procedure documents;
c. Information Technology (IT) standard operating procedures; and
d. Course materials and training guides.

2. Parties Enforcing Security Policies and Procedures

Security is no one person or department's job. Below is a highlight of the roles of various departments or groups and their role in enforcing security policies and procedures.

IOT is responsible for issuing guidance to users of State equipment and data. This may include forwarding security patches and downloads to protect technological vulnerabilities.

DCS-IT is responsible for maintaining and securing the statewide child support system and its ancillary applications.

The Security Team is a unit within DCS-IT. Among other duties, the Security Team assists the Title IV-D program in granting appropriate security clearance, providing material for security training, conducting audits, and handling security incidents.

CSB's Communications and Training Unit (CTU) is responsible for disseminating training materials, with content provided by the Security Team, to the Title IV-D program workers. CTU also maintains the library of training materials.

CSB Managers and County Security Administrators (CSAs) are responsible for administering new employee security training, administering annual security recertification training, reporting security incidents to the Security Team, and reviewing and maintaining access logs.

Title IV-D program workers are the first line of defense in securing confidential information. Workers are responsible for reading and/or viewing security training materials and abiding by the clean desk policy. The clean desk policy means that any confidential information not in use is secured and kept out of view of anyone not authorized to view the confidential information.

REFERENCES

- **IC 4-1-11-3**: "Personal information"
- **26 U.S.C. § 6103**: Confidentiality and disclosure of returns and return information
- **45 C.F.R. § 303.21**: Safeguarding and disclosure of confidential information
- **IRS Publication 1075**: Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information

PROCEDURE

N/A

FORMS AND TOOLS

N/A

FREQUENTLY ASKED QUESTIONS

N/A

RELATED INFORMATION

N/A

REVISION HISTORY

Version	Date	Description of Revision
Version 1	10/31/2022	New Section created upon review of Chapter 18 and updated Publication 1075 information.