	INDIANA DEPARTMENT OF CHILD SERVICES TITLE IV-D POLICY MANUAL	
	Chapter 18: Confidentiality and Security	**Effective Date: 5/9/19**
	Section 6: Electronic Device and Digital Media Security	**Version: 1.0** **Revision Date: 5/8/19**

BACKGROUND

N/A

POLICY

The Child Support Bureau (CSB), Title IV-D Prosecutor, and Clerk of Courts (collectively referred to as the Title IV-D agency) shall observe safeguards for protecting confidential information, with the minimum standard for the safeguards being the federal regulations governing the safeguarding of information.[1] These safeguards include security requirements which are further outlined in the following federal documents:

1. Internal Revenue Service – Publication 1075;
2. Social Security Administration – Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration; and
3. Office of Child Support Enforcement (OCSE) – Security Agreement.

The Child Support Bureau (CSB) shall have administrative, technical, and physical safeguards to insure the security of the statewide child support system used by the Title IV-D Program and to protect against anticipated threats or hazards to the statewide child support system's security, integrity, or access.[2] Additionally, the CSB shall have safeguards in effect concerning the integrity, accuracy, completeness of, access to, and use of data in the statewide child support system.[3]

These safeguards shall include:

1. Written policies concerning access and sharing data;[4]
2. System controls, such as passwords or blocking certain fields, to ensure adherence to written policies;[5]
3. Routine monitoring, such as through audit trails and feedback mechanisms, of access to and use of the statewide child support system to guard against and promptly identify unauthorized access or use;[6]
4. Procedures to ensure all personnel having access to confidential data are informed of applicable requirements and penalties and are trained in security procedures;[7] and

[1] 45 C.F.R. § 303.21(b); IC 31-25-4-21(a)
[2] IC 4-1-6-2(l)
[3] 42 U.S.C. § 654a(d); 45 C.F.R. § 307.13(a)
[4] 42 U.S.C. § 654a(d)(1)
[5] 42 U.S.C. § 654a(d)(2)
[6] 42 U.S.C. § 654a(d)(3); 45 C.F.R. § 307.13(b)
[7] 42 U.S.C. § 654a(d)(4); 45 C.F.R. § 307.13(c)

5. Administrative penalties, including dismissal from employment, for unauthorized access to, or disclosure or use of, confidential data.[8]

The written policies shall include:

1. Access to and use of data is only permitted to the extent necessary to carry out the Title IV-D functions;[9] and
2. Specifications as to the data that may be used and the personnel permitted access to such data.[10]

The OCSE Security Agreement prohibits Federal Parent Locator Service (FPLS) and confidential child support program information from being copied to and stored on digital media unless encrypted at the disk or device level in accordance with FIPS 140-2.[11] This includes copying information to or storing information on CDs and flash drives.

Further, the Indiana Office of Technology prohibits storing state owned information on non-state owned computers, flash drives, CDs, or other digital media.[12] The Title IV-D Prosecutor and Clerk of Courts are permitted to store state owned information on county owned servers pursuant to the cooperative agreement with the CSB.

REFERENCES

- **IC 4-1-6-2**: Personal information system
- **IC 31-25-4-21**: Confidential information; safeguards; necessary disclosures
- **42 U.S.C. § 654a**: Automated data processing
- **45 C.F.R. § 307.13**: Security and confidentiality for computerized support enforcement systems in operation after October 1, 1997
- **IRS Publication 1075**: Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information

PROCEDURE

The County Security Administrator (CSA) must review statewide child support system user IDs quarterly to determine:

1. Is the worker still employed; and
2. Does the worker still need that level of access.

If the CSA finds that a worker on the user ID list is no longer employed or whose access need has changed, the CSA immediately contacts the CSB Help Desk to have the worker's access changed.

When a computer is not in use, it should be locked and password protected. Computers are to be set to have a 15 minute time out function so that the computer automatically locks when no activity has occurred after 15 minutes. Passwords to access computers or computer programs are not to be shared.

---

[8] 42 U.S.C. § 654a(d)(5)
[9] 42 U.S.C. § 654a(d)(1)(A)
[10] 42 U.S.C. § 654a(d)(1)(B)
[11] OCSE Security Agreement, Section II.B.10
[12] Indiana Resources Use Agreement Section 3

When the Title IV-D Program will be disposing of an electronic device or digital media containing confidential information, including Federal Tax Information (FTI) and Personal Identifiable Information (PII), the agency shall:

1. Sanitize the device or media prior to disposal or release for reuse using IRS-approved sanitization techniques;
2. Employ sanitization mechanisms commensurate with the security category or classification of the information; and
3. Review, approve, track, document, and verify media sanitization and disposal actions. The tracking and documenting actions include:
    a. Personnel who reviewed and approved the sanitization and disposal;
    b. Types of media sanitized;
    c. Sanitization methods used;
    d. Date and time of the sanitization actions;
    e. Personnel who performed the sanitization;
    f. Verification actions taken;
    g. Personnel who performed the verification; and
    h. Disposal action taken.[13]

Disposal of an electronic device or digital media must also comply with all applicable state and county records retention policies.[14]

FORMS AND TOOLS

1. How to Review ISETS Worker Status and Profile
2. Information Resources Use Agreement (IRUA)
3. IRUA for County Users
4. OCSE Security Agreement
5. User Access Requests – CSA Forms Desktop Guide
6. Users Security Guide

FREQUENTLY ASKED QUESTIONS

N/A

RELATED INFORMATION

N/A

[13] Publication 1075, Sections 9.3.10.6 and 9.4.7
[14] Publication 1075, Section 9.3.10.6