	INDIANA DEPARTMENT OF CHILD SERVICES TITLE IV-D POLICY MANUAL	
	Chapter 18: Confidentiality and Security	**Effective Date: 10/31/2022**
	Section 6: Electronic Device and Digital Media Security	**Version: 1.1** **Revision Date: 10/31/2022**

BACKGROUND

N/A

POLICY

The Child Support Bureau (CSB), Title IV-D Prosecutor's Office, and Clerk of Courts (collectively referred to as the Title IV-D program) observes 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.

CSB has administrative, technical, and physical safeguards to ensure 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, CSB has safeguards in effect concerning the integrity, accuracy, completeness of, access to, and use of data in the statewide child support system.[3]

These safeguards 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(12)
[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 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 pursuant to current FIPS requirements.[11]

The Indiana Office of Technology (IOT) has additional safeguards regarding the storage of data, which includes Federal Tax Information (FTI) and/or Personal Identifiable Information (PII), as outlined in the Indiana Resources Use Agreement that users sign as part of their annual security training. By extension of the cooperative agreement, the Title IV-D Prosecutor's Office and Clerk of Courts are permitted to access or store this information on official office equipment using State-issued credentials.

IOT has also authorized that the storage of data may be done on its approved cloud storage providers of OneDrive for Business or Syncplicity.[12] CSB utilizes OneDrive for Business as its cloud storage depository for data obtained within the Title IV-D program.

IOT categorizes a mobile device to be any mobile phone, smartphone, tablet, or hybrid device.[13] A smartphone is a mobile device that includes cellular voice, messaging, scheduling, email, and internet capabilities.[14] A tablet is a mobile device that has a touchscreen display larger than that of a smartphone and includes messaging, scheduling, email, and internet capabilities, with no cellular voice capabilities.[15] The mobile device must have the highest level of protection practical and must employ encryption mechanisms to ensure that confidential information is protected and may not be accessed if the mobile device is lost or stolen.[16]

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

[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.11
[12] IOT-CS-OPS-001: OneDrive for Business OPS-001
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] Publication 1075, Section 2.B.5

- **IRS Publication 1075**: Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information

PROCEDURE

1. Passwords

   When a computer is not in use, it is to 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.[17] Passwords to access computers or computer programs are not to be shared.

2. Maintenance and Replacement

   When the Title IV-D program will be maintaining, repairing, or replacing an electronic device or digital media containing confidential information, including FTI and/or PII, the agency shall:
   a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
   b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;
   c. Require that an agency assigned official explicitly approve the removal of the system or system components from the organizational facilities for off-site maintenance, repair, or replacement;
   d. Sanitize equipment to remove all FTI and/or PII from associated media prior to removal from the agency's facilities for off-site maintenance or repairs;
   e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
   f. Include the following information in organizational maintenance records:
      1) Date and time of maintenance;
      2) Name of the individual performing the maintenance;
      3) Name of escort, if necessary;
      4) A description of the maintenance performed; and
      5) A list of equipment removed or replaced (including identification numbers, if applicable).[18]

3. Disposal

   When the Title IV-D program will be disposing of an electronic device or digital media containing confidential information, including FTI and/or PII, the agency shall:
   a. Sanitize the device or media prior to disposal or release for reuse using IRS-approved sanitization techniques;
   b. Employ sanitization mechanisms commensurate with the security category or classification of the information; and

[17] Publication 1075, Section 4.1 AC-11
[18] Publication 1075, Section 4.9 MA-2

c. Review, approve, track, document, and verify media sanitization and disposal actions. The tracking and documenting actions include:
    1) Personnel who reviewed and approved the sanitization and disposal;
    2) Types of media sanitized;
    3) Sanitization methods used;
    4) Date and time of the sanitization actions;
    5) Personnel who performed the sanitization;
    6) Verification actions taken;
    7) Personnel who performed the verification; and
    8) Disposal action taken.[19]

Disposal of an electronic device or digital media must also comply with all applicable State and county records retention policies.[20]

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. Users Security Guide
6. Federal Information Processing Standards Publication 140-3
7. Policy and Procedures for Use of Personally Owned Mobile Devices to Access the Information Resources of Indiana State Government: A Semi-managed BYOD Program
8. IOT-CS-OPS-001: OneDrive for Business OPS-001

FREQUENTLY ASKED QUESTIONS

N/A

RELATED INFORMATION

N/A

REVISION HISTORY

Version	Date	Description of Revision
Version 1	05/09/2019	Final Approved Version
Version 1.1	10/31/2022	Updated hyperlinks and renumbered. Reviewed for accuracy pursuant to IRS Publication 1075.

[19] Publication 1075, Section 4.10 MP-6
[20] Publication 1075, Section 4.10 MP-1