	INDIANA DEPARTMENT OF CHILD SERVICES TITLE IV-D POLICY MANUAL	
	Chapter 18: Confidentiality and Security	**Effective Date: 10/31/2022**
	Section 7: Remote Access for an Alternate Work Site	**Version: 1** **Revision Date: 10/31/2022**

BACKGROUND

Remote access is defined as access to agency systems (or processes acting on behalf of users) communicating through external networks such as the internet.[1] The access originates from outside an agency network and enters the network through an internet gateway.

POLICY

If the confidentiality of Federal Tax Information (FTI) can be adequately protected, telework sites such as an employee's home or other non-traditional work sites may be used.[2] All FTI safeguards and protections that apply while working in an office will also apply to employees while working offsite or remotely.[3]

Ultimately, the decision to offer non-traditional work sites for its employees lies with the individual office within the Title IV-D program (collectively the Child Support Bureau (CSB), Title IV-D Prosecutor's Office, and Clerk of Courts). Individual offices within the Title IV-D program may also issue additional policies and procedures governing telework for its employees.

REFERENCES

- **IC 31-25-4-21**: Confidential information; safeguards; necessary disclosures
- **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

1. Remote Access to the State Network

   The use of encrypted virtual private networks (VPN) for network connections between an agency-controlled endpoint and non-agency-controlled endpoint, may be treated as an internal network with respect to the protecting the confidentiality and integrity of information that is traversing the network.[4] The Indiana Office of Technology (IOT) will be the sole provider of remote access to the State network. VPN and Citrix are the only type of remote connections authorized for State network access. IOT requires that multi-

[1] Publication 1075, Section 4.7 IA-2
[2] Publication 1075, Section 2.B.7
[3] 45 C.F.R. § 307.13(a); IC 31-25-4-21(a); Publication 1075, Section 2.B.7
[4] Publication 1075, Section 4.7 IA-2

factor authentication (MFA) be utilized for each remote connection before permitting access to the State network.

FTI must not be received, processed, stored, accessed, or transmitted to IT systems located outside of the legal jurisdictional boundary of the United States (outside of the United States, its territories, embassies, or military installations).[5]

2. Equipment

Individual offices within the Title IV-D program must retain ownership and control for all hardware, software, and end-point equipment, such as an employee's computer, connecting to public communication networks where these are present at alternate work sites.[6] By extension of the cooperative agreement, the Title IV-D Prosecutor's Office and Clerk of Courts are permitted to access the State network on official office equipment using State-issued credentials. The equipment must have the highest level of protection practical and must employ encryption mechanisms to ensure that FTI may not be accessed if the equipment is lost or stolen.[7]

3. Physical Security

An employee must have a specific room or area in a room that has the appropriate space and facilities for his or her work.[8] Individual offices within the Title IV-D program must ensure an employee has access to locking file cabinets or desk drawers.[9] An employee also must have a way to communicate with managers or other members of his or her Title IV-D office if security problems arise.[10]

As part of security awareness and training, CSB disseminates rules and procedures to ensure that employees do not leave computers or other FTI unprotected.[11]

FORMS AND TOOLS

1. Information Resources Use Agreement (IRUA)
2. IRUA for County Users
3. OCSE Security Agreement
4. Users Security Guide
5. Federal Information Processing Standards Publication 140-3
6. Policy and Procedures for Use of Personally Owned Mobile Devices to Access the Information Resources of Indiana State Government: A Semi-managed BYOD Program

FREQUENTLY ASKED QUESTIONS

N/A

[5] Publication 1075, Section 2.C.7
[6] Publication 1075, Section 2.B.7.1
[7] Publication 1075, Section 2.B.5
[8] Publication 1075, Section 2.B.7.1
[9] Publication 1075, Section 2.B.7.1
[10] Publication 1075, Section 2.B.7.1
[11] 45 C.F.R. § 307.13(c); Publication 1075, Section 2.B.7.3

RELATED INFORMATION

Chapter 18: Confidentiality and Security, Section 3: Accessing and Protecting Federal Tax Information (FTI)
Chapter 18: Confidentiality and Security, Section 6: Electronic Device and Digital Media Security
Chapter 18: Confidentiality and Security, Section 10: Reporting a Security Incident

REVISION HISTORY

Version	Date	Description of Revision
Version 1	10/31/2022	Final Approved Version