	INDIANA DEPARTMENT OF CHILD SERVICES TITLE IV-D POLICY MANUAL	
	Chapter 18: Confidentiality and Security	**Effective Date: 5/9/19**
	Section 5: County Security Administrator (CSA) Duties	**Version: 1.0** **Revision Date: 5/8/19**

BACKGROUND

Each Title IV-D Prosecutor's office and each Clerk of Courts' office has a County Security Administrator (CSA). The CSA is the main security point of contact for the Child Support Bureau (CSB) Security Team and the CSB Help Desk.

POLICY

The responsibilities of the CSA include employee and contractor security training, limiting and auditing access, record keeping, and reporting security incidents.

REFERENCES

N/A

PROCEDURE

1. Employee Security Training

   The CSA is responsible for ensuring all new employees and contractors receive Federal Tax Information (FTI) training prior to receiving access to FTI and all employees and contractors complete the annual FTI recertification training. The self-led training on the Child Support Resources (CSR) website is appropriate for both the new and recertification training. The best practice is for the CSA to be present with the new employee or contractor when taking the self-led training to answer office specific questions such as where logs are kept or where the shredder or secured shred box is located.

2. Limiting and Monitoring Access

   The CSA is responsible for completing the Disable/Enable/Delete ISETS or CSR User ID Request form that is then submitted to the CSB Help Desk for the following user ID maintenance:
   a. Requesting user IDs for new workers;
   b. Submitting modification of user IDs when user information changes;
   c. Ensuring that user IDs are disabled when a worker will be absent from the office for two (2) or more weeks;
   d. Ensuring that user IDs are enabled when a worker returns to work from an absence of two (2) or more weeks; and
   e. Promptly requesting revocation of all user access when the worker leaves employment.

The CSA is also responsible for limiting physical access. The CSA ensures the office is using a two (2) barrier method of protecting FTI.[1] In conjunction with IT staff, the CSA ensures that the office computer systems, fax, copier, and scanner meet the security requirements prescribed by the Office of Child Support Enforcement (OCSE); Social Security Administration (SSA); Department of the Treasury, Internal Revenue Service (IRS); Indiana Office of Technology (IOT), and CSB. The CSA also maintains records of keys and combinations and the staff who have access to those keys and combinations.

3. Record Keeping

   The CSA is responsible for maintaining the required FTI logs including the Authorized Access List, Receipt-Destruction/Distribution Log, and Visitor Security Access Log.[2]

4. Reporting Security Incidents

   Whenever a staff member of a Title IV-D Prosecutor's office or Clerk of Courts' office believes FTI or Personal Identifiable Information (PII) may have been accessed by or disclosed to an unauthorized person, the staff member is to immediately notify the CSA. It is then the CSA's responsibility to begin the reporting procedures as stated in Section 9 of this Chapter.

FORMS AND TOOLS

1. Add Existing CSR Users to Data Warehouse
2. Completing the License Suspension User Access Request
3. County User Information Packet
4. Create ISETS/CSR User ID Request
5. CSA FTI and Security Smart Guide
6. Disable/Enable/Delete ISETS or CSR User ID Request
7. FTI Awareness/Training Record
8. Modify Existing ISETS, CSR, DWH or Email Information Request
9. Panoptic Request Form
10. User Access Requests CSA Forms Desktop Guide

FREQUENTLY ASKED QUESTIONS

N/A

RELATED INFORMATION

N/A

[1] See Section 3 of this Chapter for the two (2) barrier method requirements.
[2] See Section 3 of this Chapter for more detailed information on FTI logs.