	INDIANA DEPARTMENT OF CHILD SERVICES TITLE IV-D POLICY MANUAL	
	Chapter 18: Confidentiality and Security	**Effective Date: 10/31/2022**
	Section 10: Reporting a Security Incident	**Version: 1.1** **Revision Date: 10/31/2022**

BACKGROUND

The Child Support Bureau (CSB) shall observe all possible safeguards with the minimum standard for such safeguards to be federal regulations governing the safeguarding of information under the Title IV-D program.[1] This requirement extends to the Title IV-D Prosecutor's Offices and Clerks of Courts through the cooperative agreement with CSB to carry out the functions of the Title IV-D program.

POLICY

Among the federal requirements governing the safeguarding of information is that the Title IV-D program has a written policy stating the actions that will be taken upon discovering an improper inspection or disclosure of Federal Tax Information (FTI) or Personal Identifiable Information (PII), such as through a data incident or data breach.[2] A data incident is an actual or imminent event that jeopardizes the integrity, confidentiality, or availability of an information system.[3] A data incident also includes a violation of law or a violation of security or acceptable use policies or procedures.[4] A data incident involving loss, theft, or inadvertent disclosure of FTI is a data breach.[5] This involves a person other than an authorized user accessing, or potentially accessing, FTI or an authorized person accessing, or potentially accessing, FTI for an unauthorized purpose.[6]

Examples of a data breach include, but are not limited to, the following:

1. A laptop or portable storage device containing FTI is lost or stolen;
2. An email is sent containing FTI;
3. Documents containing FTI are lost or stolen during transit;
4. An unauthorized person overhears authorized personnel discussing FTI;
5. An authorized user accesses FTI for an unauthorized purpose;
6. A network intrusion, an attack exploiting website vulnerabilities, or an attack executed through an email message or attachment on a system that maintains FTI;
7. An oral disclosure of FTI to a person who is not authorized to receive that information; and
8. Inadvertent disclosure of FTI on a public website.[7]

[1] IC 31-25-4-21(a)
[2] Publication 1075, Section 1.8.2
[3] Publication 1075, Section 1.8.1.1
[4] Publication 1075, Section 1.8.1.1
[5] Publication 1075, Section 1.8.1.2
[6] Publication 1075, Section 1.8.1.2
[7] Publication 1075, Section 1.8.1.2

REFERENCES

- **IC 31-25-4-21**: Confidential information; safeguards; necessary disclosures
- **IRS Publication 1075**: Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information

PROCEDURE

An employee who becomes aware of an incident is to report the incident to the employee's supervisor. If the incident occurred in a county office, it is also reported to the County Security Administrator (CSA). The supervisor and/or CSA reports the incident to the CSB Security Team promptly.

Any actual or suspected incident in which FTI, PII, or other confidential information may have been accessed by an unauthorized person is to be reported. All suspected or actual breaches or unauthorized disclosures of FTI, Social Security Administration (SSA) provided PII, Office of Child Support Enforcement (OCSE) provided data, or other confidential information must be reported within one (1) hour of the discovery of the security incident.

The CSB Security Team has created the Security Incident Report Form (FTI & PII) to facilitate reporting incidents. This form contains specific contact information and instructions. Details of the incident or breach known at the time of the report that must be reported include, but are not limited to:

1. Name of the agency and the point of contact for resolving the data incident including the person's contact information;
2. Date and time the incident or breach occurred;
3. Date and time the incident or breach was discovered;
4. How the incident or breach was discovered;
5. Description of the incident or breach and the data involved, including specific data elements if known;
6. Potential number of records involved (if a specific number is unknown, then provide a range if possible);
7. Address where the incident or breach occurred;
8. Information technology involved (such as laptop, server, or mainframe);
9. Whether the incident involved unauthorized access or disclosure by an agency employee; and
10. If criminal prosecution is not pursued, whether a disciplinary or adverse action will be proposed against the agency employee involved in the incident or breach.[8]

Immediate notification of a potential incident is more important than the completeness of a security incident report.[9] However, additional information shall be provided as soon as it is available.[10] Any internal investigations are not to delay timely reporting.[11]

The CSB Security Team will notify the appropriate external agencies of security incidents according to each agency's reporting requirements:

[8] Publication 1075, Section 1.8.3
[9] Publication 1075, Section 1.8.3
[10] Publication 1075, Section 1.8.3
[11] Publication 1075, Section 1.8.4

1. For any security incident, the Indiana Office of Technology's Chief Information Security Officer and U.S. Computer Emergency Readiness Team;
2. For incidents involving FTI, the Treasury Inspector General for Tax Administration (TIGTA) and IRS Office of Safeguards;[12]
3. For incidents involving SSA provided PII, the SSA's National Network Service Center (NNSC);
4. For incidents involving OCSE, including FPLS, provided PII, the FPLS Information System Security Office;
5. For incidents involving Social Security numbers or certain other PII, the Indiana Attorney General; and
6. For incidents involving protected health information (PHI), the U.S. Department of Health and Human Services.

When a disciplinary or adverse action is proposed against the employee responsible for a security incident involving unauthorized access or disclosure of FTI or a Social Security number, written notice must be sent to the person whose information was accessed or disclosed.[13] This notice must include the date of the unauthorized access or disclosure and the rights of the person.[14] If the security incident occurred in a county office, it is the responsibility of the county office to notify the person. If the security incident occurred at CSB, it is CSB's responsibility to notify the person. CSB must affirm to the IRS Office of Safeguards when this notice has been provided to the person.[15]

CSB will track and document security incidents.[16] This includes post-incident review, which may be done in conjunction with the office where the incident occurred, to ensure the policies and procedures provide adequate guidance.[17] Any deficiencies in policies and procedures will be resolved as soon as practical and additional training will be provided upon implementation of updated policies and procedures.[18]

FORMS AND TOOLS

1. CSA FTI and Security Smart Guide
2. Security Incident Report Form (FTI & PII)

FREQUENTLY ASKED QUESTIONS

N/A

RELATED INFORMATION

CSB will conduct an incident response test at least annually to determine incident response effectiveness and document the results.[19]

[12] Publication 1075, Section 1.8.2-1.8.4
[13] Publication 1075, Section 1.8.5
[14] Publication 1075, Section 1.8.5
[15] Publication 1075, Section 1.8.5
[16] Publication 1075, Section 1.8.4
[17] Publication 1075, Section 1.8.4
[18] Publication 1075, Section 1.8.4
[19] Publication 1075, Section 1.8.4

REVISION HISTORY

Version	Date	Description of Revision
Version 1	05/09/2019	Final Approved Version
Version 1.1	10/31/2022	Updated hyperlinks. Reviewed for consistency. Renumbered Section. Updated Publication 1075 information.