



**JUSTICE CABINET  
DEPARTMENT OF  
JUVENILE JUSTICE  
POLICY AND PROCEDURES**

**REFERENCES:**

**CHAPTER: Administration**

**AUTHORITY: KRS 15A.065**

**SUBJECT: Potential Data Breaches or  
Personally Identifiable Information**

**POLICY NUMBER: DJJ 144**

**TOTAL PAGES: 2**

**EFFECTIVE DATE: November 30, 2018**

**APPROVAL: Carey D. Cockerell**

**, COMMISSIONER**

**I. POLICY**

The Department of Juvenile Justice (DJJ) shall maintain all Social Security or personally identifiable information in a confidential and secure manner. If a suspected breach has occurred, the department staff shall rectify the situation pursuant to the Information Exchange Agreement between the Social Security Administration and DJJ.

**II. APPLICABILITY**

This policy shall apply to all staff, volunteers, contractors, facilities, and offices of the Department.

**III. DEFINITIONS**

Refer to Chapter 100.

**IV. PROCEDURES**

- A. If there is a suspected breach, security breach, security incident, security violation, personally identifiable information (PII), or loss of Social Security Administration (SSA) provided information, contact your supervisor and the Information Systems Branch Manager or designee immediately.
- B. The Information Systems Branch Manager or designee responsible for system security must notify the SSA Systems Security Contact within one hour.
- C. If, for any reason, the responsible State official or delegate is unable to notify the SSA Systems Security Contact within one hour, the responsible State Agency official or delegate must report the incident by contacting SSA's

<b>POLICY NUMBER</b> <b>DJJ</b>	<b>EFFECTIVE DATE</b> <b>11/30/2018</b>	<b>PAGE NUMBER</b> <b>2 of 2</b>
------------------------------------	--	-------------------------------------

National Network Service Center (NNSC) toll free at 877-697-4889 (select “Security and PII Reporting” from the options list).

- D. If the SSA’s National Network Services Center is to be contacted instead of the SSA Regional Office Contact or the SSA Systems Security contact, the caller shall contact the following individual:

Brooks Hansen  
IT Specialist/ATL Region Data Exchange  
Center for Automation, Security and Integrity  
Email: Brooks.Hansen@ssa.gov

(205) 801-1819      Office  
(205) 530.1515      Telework Days

1. The caller must have the name, email, and phone number of the SSA Systems Security Contact or the NNSC will not take the report.
  2. In addition to the Social Security Administration, the Information Systems Branch Manager or designee shall also notify:
    - a. The Commissioner of the Kentucky State Police
    - b. The Auditor of Public Accounts
    - c. The Attorney General
    - d. The Secretary of Finance or designee
    - e. Notify the Commonwealth Office of Technology
    - f. Notify the CHFS OATS Security Team
- E. When reporting a breach, the Information Systems Branch Manager shall use the Attachment 5 (PII Loss Reporting Worksheet) of the Information Exchange Agreement between the Social Security Administration and the Department of Juvenile Justice.

**V. MONITORING MECHANISM**

- A. The Fiscal Branch Manager or designee shall review and analyze any system breaches at the time of the breach and resolve such breach in accordance with the Information Exchange Agreement between the Social Security Administration.
- B. The Fiscal Branch Manager or designee shall implement any system changes needed to resolve such breaches and address any concerns for future processing.
- C. The Fiscal Branch Manager or designee shall convene a committee annually to analyze the current system security for the purpose of quality improvement.