Minnesota Department of Corrections

Policy:	**105.230**
Title:	**Criminal Justice Data Network Misuse and Discipline**
Effective Date:	**1/2/18**

PURPOSE: To ensure agency use of the Federal Bureau of Investigation (FBI) National Crime Information Center (NCIC) is in accordance with the NCIC security policy, and to provide written procedures to address NCIC security policy violations.

APPLICABILITY: Minnesota Department of Corrections (DOC); department-wide

DEFINITIONS:
Criminal Justice Data Communication Network – as defined in Policy 105.205, "Computerized Information Resources Security."

Terminal agency coordinator/remote administrator – a designated DOC staff member serving as liaison to the Minnesota Bureau of Criminal Apprehension (BCA) who has the ability to add and disable users and is responsible to update training and certification for DOC users of the PS portals 100 browser-based public safety workstation (the system in which the Criminal Justice Data Communications Network is operated).

PROCEDURES:

A. The department of corrections (DOC) creates, uses, maintains, stores, preserves, and disposes of information retrieved from the Federal Bureau of Investigation's (FBI's) National Crime Information Center (NCIC) and the National Law Enforcement Telecommunications System (NLETS) in accordance with the NCIC security policy.

B. If the DOC Criminal Justice Data Communications Network (CJDN) terminal agency coordinator/remote administrator (DOC TAC) becomes aware of an employee using a CJDN terminal, CJDN terminal generated information, CJDN equipment, or CJDN access in a manner that is not in accordance to the DOC's policy or NCIC policy and the problem is deemed:
   1. Operator error or substandard job performance, the DOC TAC must:
      a) Contact the employee;

      b) Advise of the problem; and

      c) Provide additional training.

   2. Greater than mere operator error or substandard job performance and additional training has not corrected user issues, the DOC TAC must:
      a) Submit a report to the user's immediate supervisor and the office of special investigations (OSI) assistant director – investigations, and

      b) Suspend the employee's CJDN access until the supervisor conducts an investigation pursuant to procedure C (below).

      c) To include evidence the employee is performing this action as a result of intentional misconduct that may be in violation of state or federal statute:

(1) Submit a report to the OSI assistant director – investigations for review pursuant to procedure D (below); and

(2) In certain cases when criminal intent is involved, or the actions involved have impacted or may impact more than just the DOC, the DOC TAC may (after review by the OSI chief deputy) forward the report to the Minnesota Department of Public Safety control terminal operator (CTO) and/or to the FBI/NCIC criminal justice information services.

C. Supervisor investigations of CJDN use

1. The immediate supervisor must conduct an investigation in accordance with Policy 103.225, "Employee Investigation and Discipline Administration."

2. If the investigation does not substantiate that the employee was in violation of DOC policy or NCIC policy, the immediate supervisor must contact:
   a) The OSI assistant director – investigations; and
   b) The DOC TAC requesting to reinstate the employee's CJDN terminal access.

3. If the investigation substantiates that the employee was in violation of DOC policy or NCIC policy, the immediate supervisor:
   a) May take disciplinary action may be taken against the employee in accordance with applicable labor agreements; and
   b) Must contact the DOC TAC to request continued denial of CJDN terminal access to the employee. Denial of access remains until the DOC TAC is directed by the OSI assistant director – investigations to change this status.

4. All investigatory documents are retained by human resources according to approved retention schedules.

D. OSI assistant director – investigations review and investigation of CJDN use

1. If the OSI assistant director – investigations deems the conduct not to be criminal, the OSI assistant director – investigations reports back to the supervisor and the DOC TAC to recommend further supervisory investigation in regard to possible policy violations, further training, and/or reinstatement of the employee's CJDN terminal access.

2. If the misconduct is deemed to be criminal, the OSI assistant director – investigations must report the behavior to the appropriate assistant or deputy commissioner, human resources management staff, and warden (if applicable) to determine the next steps.

3. All completed OSI case files and applicable evidence must be retained by OSI according to approved retention schedules.

INTERNAL CONTROLS:

A. Supervisor investigatory documents are retained by the human resource department according to approved retention schedules.

B. Completed OSI case files and applicable evidence are retained by OSI according to approved retention schedules.

ACA STANDARDS: None

REFERENCES: Policy 105.205, "Computerized Information Resources Security"
Policy 107.100, "Internal Affairs – Office of Special Investigations"
Policy 103.225, "Employee Investigation and Discipline Administration"
NCIC Security Policy
Minn. Stat. §§13; 43A.04, subd. 4; 609.87 through 609.891, and 241.01

REPLACES: Policy 105.230, "Criminal Justice Data Network Misuse and Discipline," 2/2/16. All facility policies, memos, or other communications whether verbal, written, or transmitted by electronic means, regarding this topic.

ATTACHMENTS: None

APPROVED BY:
Deputy Commissioner, Facility Services
Deputy Commissioner, Community Services
Assistant Commissioner, Facility Services
Assistant Commissioner, Operations Support