



**Department of Human Services
Online Directives Information System**

**Index:
Revised:
Next Review:**

**POL1752
10/04/2019
10/04/2021**

**SUBJECT: Disciplinary Measures for Misuse of GCIC/NCIC
Criminal Justice Information**

POLICY:

The Department of Human Services Office of the Inspector General is liable for any violations or misuse of the criminal history process, including use and dissemination of information available via the Criminal Justice Information System (CJIS). Failure to abide by federal and state laws, federal rules and regulations, and Georgia Crime Information Center (GCIC) rules regarding access, use and dissemination of information available via the Criminal Justice Information System (CJIS) Network may result in criminal prosecution by the Department of Human Services, the Office of Inspector General, and/or administrative sanctions by the Office of Administrative Services and/or GCIC.

A. Authority

GCIC Rule 140-2-.09

B. References

Criminal Justice Information Services (CJIS) Security Policy Version 5.2, 2013
Georgia Crime and Information Center Policy Manual Rev. 2011
Georgia Crime Information Council Rules, October 2007

C. Applicability

Any employee authorized by OIG to capture and/or transmit fingerprints via an electronic fingerprinting machine or who accesses the GCIC Network Terminal.

D. Definitions

Terminal Agency Coordinator (TAC): The person designated by an agency head to serve as a liaison between the agency head and the GCIC for complying with GCIC and NCIC/NLETS Policies, Rules and Regulations (GCIC Council Rule 140-1-.02).

Criminal History Information: Records that include direct responses from GCIC and National Crime Information Center (NCIC) received as a result of the submission of electronic fingerprints or GCIC Query Terminal responses.

E. Responsibilities

According to GCIC:

1. All local agencies **must** have disciplinary procedures that address violations of GCIC Rules, Georgia law, or federal rules and regulations relative to the GCIC/NCIC Criminal Justice Information System (GCIC Rule 140-2-.09).
2. The agency head will take appropriate disciplinary action against any employee who has violated or misused criminal history information, including

use and/or dissemination, to prevent further policy violations.

3. All security violations must be investigated by the agency and reported, in writing, to the GCIC Deputy Director.
4. The sanctions to be administered by the Agency may include, but are not limited, to:
 - a. Mandatory retraining and/or recertification of the Terminal Agency Coordinator (TAC) by requiring attendance at another TAC class sponsored by GCIC, as well as completion of certain parts of the CJIS workbook, even if the TAC is not a certified operator.
 - b. Mandatory retraining and/or recertification of a terminal operator who should complete an entire workbook or specific portions of a workbook, and subsequently pass another full certification test.
 - c. Probation or suspension/revocation of the operator's User ID/password or TAC certification for GCIC accessdatory retraining in the form of another Security and Integrity Training Update class. After completion of any training, the operator must read and sign an updated GCIC Awareness Statement.
 - e. Restriction on processing criminal history requests until mandatory retraining and/or recertification is completed.
 - f. Written reprimand, suspension, termination from the agency, and possible criminal prosecution.
5. If the disciplinary action taken by the Agency against an employee is not appropriate for the violation, the GCIC reserves the right to implement additional sanctions. Additional sanctions may include termination of criminal history records access and state and/or federal criminal penalties.
6. If the individual's violation is major, or the **individual** has had repeated violations, the GCIC Deputy Director will notify the Peace Officers Standards and Training (P.O.S.T.) Council of the GCIC violations and request that P.O.S.T. take appropriate action.
7. If the Agency's violation is major, or the **Agency** has had repeated violations, the GCIC Deputy Director may notify the Georgia Public Safety Board of the GCIC violations and recommend suspension or termination of the agency's CJIS Network Access

F. History

Policy 1750, last reviewed 10/04/2019

G. Evaluation

The OIG BIU Manager/Supervisor evaluates this policy by:

1. Completing quarterly internal audits to ensure responsibilities, certification, and dissemination are performed accurately and efficiently by each employee.
2. Passing any audit with no findings.