COMPUTER – CRIMINAL JUSTICE DATABASE ACCESS

POLICY:

It is the policy of the Omaha Police Department (OPD) that OPD employees only access and/or disclose information from criminal justice databases for legitimate law enforcement purposes.

PROCEDURE:

I. General

A. Inquiries through criminal justice record or information systems shall only be for legitimate law enforcement purposes.

1. This includes but is not limited to NCIC (National Crime Information Center), NCJIS (National Criminal Justice Information System), OPD Records Management System (RMS), SAFE Evidence System, IMS – Douglas County Mainframe, and the Nebraska DMV (Department of Motor Vehicles) Database.

B. Requests for information shall be referred to the appropriate Unit or Section.

C. Employees are strictly prohibited from using criminal justice databases for curiosity or personal use.

D. OPD employees who operate criminal justice databases shall be trained and certified in the use of the systems within six (6) months of assignment.

E. Basic security awareness training shall be completed by all OPD employees who will access criminal justice information/databases within six (6) months of assignment, and biennially thereafter.

1. The certification process is the responsibility of the OPD Administrative Information Manager.

F. The FBI requires that all criminal justice system operators who have unescorted access in areas with criminal justice databases/information be fingerprinted and have undergone a background investigation/check. This requirement is met as all OPD employees are fingerprinted and complete a full background check pre-employment.

G. For procedures related to the security of criminal justice information see the OPD "Computer – Media Protection" policy.

II. Limiting Access

A. Unauthorized access to or routine viewing of terminals or criminal justice database/information access is prohibited.

B. OPD employees shall safeguard electronic and printed information from criminal justice databases. This includes, but is not limited to the following:

1. Lock computer screens when leaving their work area.

2. Secure printed materials when leaving their work area.

3. Properly dispose of printed information when no longer needed.

4. Do not write down or share password(s) with others.

C. OPD employees shall share criminal justice information only on a "need to know" basis.

1. Criminal justice information may be disclosed to OPD employees and agents of the OPD as needed for the performance of their duties.

2. OPD employees may exchange criminal justice information with their supervisor or in consultation with other OPD employees to enable them to be more effective in their role.

D. OPD employees shall remedy all situations that might allow for inadvertent disclosure of criminal justice information.

1. OPD employees shall not discuss criminal justice information with unauthorized people or in places where unauthorized people might possibly overhear.

2. OPD employees shall not leave criminal justice database records out on a desk or displayed on a computer screen when not being used or where people unauthorized to see the materials may view them.

III. Violations

A. If OPD employees observe unauthorized access or disclosure of information from a criminal justice database, they are to report it to their supervisor immediately. OPD employees can be considered in violation of policy for not reporting an unauthorized disclosure.

1. If an OPD employee's direct supervisor is involved in the unauthorized disclosure, they should report the violation to another supervisor.

2. If information from the FBI's Criminal Justice Information System (CJIS) is improperly disclosed, lost, or reported as not received, the following procedures shall be followed:

a. The employee shall immediately notify their supervisor and/or the OPD Information Technology Unit Manager.

b. The supervisor will communicate with the OPD Information Technology Unit Manager to notify them of the loss, disclosure, or unauthorized access of the FBI's CJIS records.

c. The OPD Information Technology Unit Manager shall ensure that a "CLEIN-NCIC Security Incident Report Form" is completed and submitted within 24 hours of discovery of the incident.

(1) The report must include a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident.

d. The OPD Information Technology Unit Manager will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of the security incident(s).

NOTE: Refer to the "Computer – Media Protection" policy for more procedures on protecting information from the FBI's CJIS.

B. All supervisors will promptly address the issue of inappropriate and inadvertent criminal justice database use with their subordinates and report any deviations to their bureau commander and the OPD Information Technology Unit Manager, who acts as the Department's Local Agency Security Officer.

1. Inquiries made for personal use, or inappropriate use or dissemination of information from any criminal justice database, can result in internal discipline, as well as penalties under Federal and State law.

2. Disciplinary actions shall be pursued in accordance with the OPD "Professional Oversight – Disciplinary Action" policy.

REFERENCES:

I. Laws

A. Nebraska Revised Statute (NRS) §29-3519 is relevant to this policy.

II. Previous OPD Orders

A. Previous General Orders: #89-18, 63-22, and 63-22 Supplement #1.

III. Accreditation Standards

A. CALEA Accreditation standard 82.1.1 is relevant to this policy.