A. PURPOSE. To provide personnel with procedures regarding the management of Criminal Justice Information System (CJIS) records and the access, storage, transport and destruction of Criminal Justice Information (CJI).

B. ACRONYMS

1. CJI – Information from a Criminal Justice Information System
2. CHRI – Criminal History Record Information
3. CJIS – Criminal Justice Information System
4. CMIS – Corrections Management Information System
5. LEIN – Law Enforcement Information Network
6. NCIC – National Crime Information Center
7. NLETS – National Law Enforcement Telecommunications System
8. OCA – Originating Complaint Number
9. ORI – Originating Agency Identification
10. SOS – Secretary of State
11. TAC – Terminal Agency Coordinator
12. LASO – Local Agency Security Officer

C. GENERAL RULES

1. CJI shall only be used for the administration of criminal justice or public safety. Any inappropriate or inadvertent disclosure and/or use of CJI will be reported to the Commander of Records & Technology.

2. CJI shall not be disseminated to an unauthorized agency, entity, or person. Authorized personnel shall protect and control CJI while stored and in transit. Appropriate safeguards shall be taken to protect CJI and limit potential mishandling or loss.

3. CJIS printouts or CJIS data shall not be released to a private party for any purpose. Personnel will control, protect, and secure CJI during transport from public disclosure.

4. A person shall not access, use, or disclose information from CJIS for personal use or gain. Personnel will not use publicly accessed computers, such as those found in hotel business centers or libraries, to access, store, or transport CJI.

5. Unless authorized by statute, rule, or policy, only those with an assigned ORI are authorized recipients of CJIS/NCIC information.

6. Any violation of CJIS rules could result in denial of access to the CJIS and the National Crime Information Center (NCIC), as well as criminal penalties.

7. Employees shall take all reasonable precautions to protect CJI in order to prevent the unintentional release of information. This includes ensuring that CJI does not remain displayed on monitors in view of unauthorized persons or when the user is away from the work station or vehicle containing a MDC.

8. All Grand Rapids Police Department (GRPD) incident reports and criminal justice records may have CJI contained in them and thus are to be treated as CJI.

9. Case files should be purged of all CHRI/NCIC data once a case is closed or when the information is no longer accurate. CJI will be securely stored within controlled areas where access is limited to authorized personnel.

    a. Physical CJI, such as printouts, CDs, and other similar items, shall be shredded using department approved and provided shredders.

    b. Electronic CJI, such as department issued computers, shall only be moved, repaired, and/or replaced at the direction of IT. Electronic CJI needing to be destroyed shall only occur at the direction of IT and will consist of the physical destruction of the electronic CJI.

10. Only those personnel who qualify, and have been trained, shall have access to CJI.

    a. The TAC/LASO shall review agency accounts annually to ensure access and privileges are commensurate with job functions and employee status.

    b. The TAC/LASO shall deactivate access accounts for employees terminated, separated, or otherwise no longer employed by the department.

D. PENALTIES

1. CJIS Policy Council Act (MCL 28.214). A person who intentionally violates the dissemination rules of MCL 28.214 is guilty of a crime as follows:

a. For a first offense, the person is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than $500, or both.

b. For a second or subsequent offense, the person is guilty of a felony punishable by imprisonment for not more than 4 years or a fine of not more than $2000, or both.

2. Driver Privacy Protection Act (MCL 257.903). Misuse of SOS records violates the Driver Privacy Protection Act.

a. A person who makes a false certification to access personal information is guilty of a felony.

b. Any individual who uses personal information for a reason other than a permissible purpose commits a felony.

E. CRIMINAL HISTORY RECORD INFORMATION (CHRI)

1. To ensure rules and regulations are followed, all criminal history record inquiries must be supported by appropriate documentation. The Grand Rapids Police Department maintains CHRI logs to document all criminal history queries. Required fields for these logs include the operator's name, requester's name and agency, appropriate purpose code, reason for the inquiry, and OCA or information directing to supporting documentation.

2. Secondary dissemination of CHRI records to the Prosecutor and Courts is allowed, but must be recorded. This can be accomplished either within the case file or for CHRIs, on the CHRI log.

3. CHRI/NCIC information is not to be retained indefinitely. Agencies are prohibited, by policy, from storing Criminal History Record Information for extended periods unless there is just cause to do so. CHRI may only be accessed for an authorized reason and used for an authorized purpose, consistent with the reason it was accessed. CHRI records shall be stored in a secure environment. CHRI may be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.

F. TRANSMISSION OF INFORMATION

1. Information received from CJIS that may be routinely transmitted via radio airwaves include all LEIN, NCIC, NLETS, SOS and CMIS

responses. The law allows for Sex Offender Registry information to be broadcast via radio transmission for identification and investigatory reasons.

2. Criminal history records shall not be routinely transmitted via radio. However, transmissions are permissible, in part, for purposes of identification or officer or public safety.

3. Faxing of CJIS/NCIC material is allowable provided the receiving fax machine is at an authorized agency and is attended by authorized staff.

4. The following items are approved to be imported from the CJIS response into police reports:

    a. SOS Response: Name, race, sex, date of birth, address, operator code, height, weight, eye color

    b. Vehicle information

5. Transmission of CJI electronically must be encrypted and may not be transmitted electronically (emailed) to anyone without a "@grand-rapids.mi.us" email address unless it has been encrypted.

G. RELEASE OF INFORMATION

1. Any employee may release a GRPD criminal justice record to a CJI authorized recipient for a criminal justice purpose (criminal investigation and/or prosecution).

2. Any request for a GRPD criminal justice record to be released for a non-criminal justice purpose or to a non-authorized CJI recipient must be submitted to the Records Unit for review and necessary redaction.

H. PERSONALLY OWNED DEVICES

1. Personnel utilizing any device purchased by the individual, and not issued by the department, shall ensure compliance with the listed conditions prior to accessing, storing, or transporting CJI.

    a. LASO approval is required prior to use

    b. Allow the LASO remote access to the device to erase as needed

c. Use good judgement before installing applications on the device

d. Advise the LASO immediately if the device is lost, stolen, or is intended for sale

e. Control wireless network and service connectivity to avoid using open or otherwise unsecure networks

f. Utilize access control measures on the device at all time, such as passwords or biometrics

2. The Commander of Records & Technology shall ensure all personally owned devices accessing CJI meet the following criteria:

a. Up to date operating systems, security patches, firmware and antivirus

b. Are configured for local device authentication

c. Using advanced authentication and encryption

d. Able to deliver built-in identify role-mapping, network access control and real-time endpoint reporting

e. Cached information erased when session is terminated

f. Personal Firewalls employed

g. Bluetooth configured as undiscoverable except as needed for pairing

h. Device is compatible with needed network protocols for accessing CJI

i. Deploy Mobile Device Management or SIM card locks and credential functions

j. Retain the ability to secure, control and remotely erase CJI from device in the event of loss, theft, or data breach

k. Enable “find my phone” service

l. Grant and manage access to CJI by personally owned devices pursuant to policy and statute

I. AUDITS AND VALIDATIONS

A. Accounts shall be validated and audited biannually.

B. Account validations and audits shall be conducted by the Commander of Records & Technology or their designee.