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 the Support Services Division.

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 which includes:

    a. Using an opaque file folder or envelope for hard copy printouts and securing in a locked briefcase or lockbox during transport outside the secured area. This includes printing out reports for court appearances.

    b. Attach a privacy statement to all electronic and paper documents.

c. Digital memory media i.e., thumb drives, flash drives, magnetic tape or disk, backup medium, optical disk, external hard drives, or digital memory card will be secured in a locked briefcase or lockbox for transport outside of the secured area or when left unattended.

d. Only view CJIS material in a secure area and ensure that unauthorized personnel are not able to observe the protected material. This includes printed reports for court appearances.

e. Do not take CJI home or when traveling unless authorized by the Grand Rapids Police Department LASO.

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 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 workstation or vehicle containing an 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 or

placed into an approved shredding container to be shredded by a department authorized contractor.

b. Electronic CJI, such as department issued computers or other items storing CJI data, 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.

c. All personnel with access to CJI shall complete CJIS training and certification prior to CJI access and complete recertification annually. TAC/LASO may require personnel to complete additional CJI training as needed.

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 violate 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.

3. Address Confidentiality Program Act (MCL 780.855).

   a. The program was created to conceal victims' addresses. This program is for victims of domestic violence, sexual assault, stalking, human trafficking, or anyone who fears that disclosure of their address increases their risk of threat or physical harm. The program protects a participant's actual physical address from being disclosed publicly. Participants receive a new official designated address. Sharing contact information for participants is highly restricted.

   b. A person that knowingly discloses confidential contact information is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than $500.00, or both.

4. Use of any department issued device shall be done in accordance with the manual of procedures, policy, and applicable law. Violation of any term may result in discipline.

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) unless prohibited by the Address Confidentiality Program Act.

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.

3. Department records, including incident reports and photographs, shall not be stored on any privately owned electronic device, nor shall department records be transmitted in any way using privately owned devices or to a privately owned device.

H. PERSONALLY OWNED DEVICES

1. Electronic communication device, described as a “department phone” or “department device”, to include any cellular phone, smartphone, connected tablet, wireless air card, wireless modem or any other modem or device with the function of electronic communication.

2. All Cellular phones, tablets, digital recorders, or other devices that are not issued by Grand Rapids Police Department shall not be used to conduct department business. Unauthorized accounts shall not be used to conduct department business.

3. Members shall not use personal email accounts to conduct department business, including sending, receiving, or storing department records. Members shall not use personal email accounts to communicate department business with any person outside the department, including witnesses, victims, suspects, prosecutors, news media, or others doing business with the department. 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.

I. DEPARTMENT ISSUED ELECTRONIC DEVICE

1. Members may carry a department device while off duty.

2. Members are allowed to use department devices to access department e-mail accounts, respond to electronic messages, perform work-related functions, and answer calls while off duty. Compensation for any work-related activity requires supervisory approval.

3. Department issued devices are issued for work related activities. Use of a department device for personal communication shall be reasonable, limited in duration and frequency, and not interfere with official work functions.

4. Department phones shall be utilized in compliance with MVC 257.602b while operating a motor vehicle (use in accordance with statutory exceptions allowed).

5. The purpose of a department-issued device is for conducting official department business and is subject to compliance with CJIS policy, audit, and use review. Use of a department issued device in an illegal or

inappropriate manner may result in discipline up to and including termination.

6. Members have no expectation of privacy regarding any communication made with or the files stored on department owned and issued devices. Administrative searches of departments devices and all contained files may be conducted as deemed necessary by department supervisors or command personnel without prior notice and without establishing probable cause or the procurement of a search warrant.

7. Members issued a department device shall maintain and monitor issued equipment while on duty and monitor when operating in an on-call capacity.

8. Members are required to routinely monitor their department device while on duty or in a callout capacity.

    a. Use of department phones for photos, video, and records are authorized as it relates to a direct work-related function (i.e., use of AXON in collecting, processing, and uploading evidence). Evidence produced or received shall not be edited and shall be submitted in its original form. Any deviation from this policy shall be documented in a report narrative.

I. APPLICATION AND MAINTENANCE

1. Deleting and uploading phone applications are to be done with authorization from the Commander of Support Services.

2. Use of department phones for photos, video, and records is authorized as it relates to a direct work-related function (i.e. use of AXON in collecting, processing, and uploading evidence in AXON).

3. The employee is responsible for care and maintenance of all devices issued to them and shall:

    a. ensure that the operating systems, security patches, firmware, and antivirus programs are up to date.

    b. Bluetooth configured as undiscoverable except as needed for pairing.

    c. retain Mobile Device Management or SIM card locks and credential functions installed on the department device.

d. ensure that “find my phone” services are always enabled.

e. return all department issued devices to Support Services Division commander at the time of separation from employment, or as directed.

f. advise the Support Services Division Commander or LASO immediately if the device is lost, stolen, or is intended for sale.

g. control wireless network and service connectivity to avoid using open or otherwise unsecure networks.

I. AUDITS AND VALIDATIONS

1. Accounts shall be validated and audited biannually.

2. Account validations and audits shall be conducted by the commander of the Support Services Division or their designee.