Series	Effective Date	Review Date	Directive Number
300 Support Services	3/3/2015	Annually	307.3
Chapter 307 - Information Systems Management			
Reviewing Office Identification			☐ New Directive ☒ Revised Revisions are in *italics*
References			

COMPUTERIZED CRIMINAL HISTORY

307.3 - 1 PURPOSE

The purpose of this directive is to specify conditions governing the release of Computerized Criminal History records information by department personnel.

307.3 - 2 POLICY

It is the policy of this department to authorize only specific members to release Computerized Criminal Record information and then only to qualified agencies or individuals. This policy provides guidelines to ensure any release of any information is consistent with all applicable city, state, and federal laws.

307.3 - 3 Computerized Criminal History Records

The Michigan Computerized Criminal History record is an automated and expanded version of those fingerprint-supported criminal history records maintained by the Michigan State Police, Records and Maintenance.

Information entered into and taken from the computerized criminal history records is highly confidential and available only on request from authorized criminal justice personnel. The Michigan State Police will make all the entries into the records, exclusively.

Information received from the Computerized Criminal History records cannot be used for anything other than the administration of criminal justice and criminal justice agency employment. Such abuses will cause the department to forfeit its privilege of using this vital source of information.

307.3 - 4 Limitations on Use and Dissemination

Dissemination and use of computerized criminal history information is limited, whether directly or through any intermediary, only to the following agencies in the discharge of their official mandated responsibilities:

1. Police agencies that are responsible for enforcement of general criminal laws;
2. Prosecuting agencies;

3. Courts;
4. Correction departments, including corrective institutions and probation departments;
5. Parole commissions and parole agencies;
6. Agencies at all governmental levels, which have as a principal function the collection and provision of fingerprint identification information;
7. Such other individuals and agencies which require Computerized Criminal History Records information to implement a state or federal statute of executive order that expressly refers to criminal conduct and contains requirements and/or exclusions expressly based upon such conduct;
8. Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice. The agreement shall specifically authorize access to data, limit the use of data to purposes for which given, and ensure that the security and confidentiality of the data is consistent with regulations;
9. Individuals and agencies for the express purpose of research, evaluative or statistical activities pursuant to an agreement with a criminal justice agency. The agreement shall specifically authorize access to data; limit the use of data to research, evaluative, or statistical purposes; ensure the confidentiality and security of the data consistent with the regulations;
10. Agencies of state or federal government which are authorized by statute or executive order to conduct investigations determining employment suitability or eligibility for security clearances allowing access to classified information; and
11. Individuals and agencies where authorized by court order or court rule.

Computerized Criminal History record information shall not be transmitted over any department radio, either through voice communication or by digital communication (via the Mobile Data Terminal System) except when it is necessary to ensure adequate safety for a law enforcement officer or the general public.

Access to computer terminals should be kept to a minimum. Therefore, the officer in charge of each terminal location shall designate only trained or certified terminal operators who shall be responsible for the physical operation of that terminal when Computerized Criminal History inquiries are made. Terminal Operators shall be certified once a year. They may miss one year of certification, but it shall not exceed two (2) years.

307.3 - 4.1 Dissemination to Outside Agencies

When an individual from an outside agency requests Computerized Criminal History record information through the use of a department terminal, the commanding officer of the concerned terminal location may, upon satisfactory verification of the individual's identity and purpose, grant the request. However, commanding officers are cautioned that sanctions for violations of the rules and regulations governing access, use and

dissemination of this information may be imposed on the agency disseminating the information even though the violation was committed by an outside individual or agency.

307.3 - 4.2 Dissemination of Raw Data from Department Records

While the police department wishes to extend all possible courtesy and cooperation to outside agencies and individuals seeking to advance the body of law enforcement and criminal justice knowledge, assistance must be limited by the necessity to preserve valuable department resources for more essential police purposes. There is also the need to respect the confidentiality of some police department data and the rights of individuals whose names may appear in department records.

In order to ensure that requests from outside agencies and individuals who conduct research projects are handled in a uniform manner and to ensure that the Detroit Police Department resources are used most efficiently in connection with such studies, the following guidelines are established:

1. Each request from outside the department to conduct a research study must be in writing and will be reviewed by Planning and *Deployment* in consultation with the commanding officer of the command from which the data will come, if applicable;
2. The researcher's parent institution must join in making the request and must sanction the research. Recommendation will be made to the Chief of Police for approval or disapproval of the request;
3. The researcher or his/her representative must conduct the actual work. The department's role will be limited to providing access to data and to necessary informational discussions concerning the subject matter of the project;
4. The department retains the right to determine what data will be provided and to withhold specific information when necessary;
5. Work must be done on department premises and no documents or copies may be removed from the work site;
6. The use of department copying equipment by outside researchers shall not be authorized unless it is for the benefit of the Detroit Police Department;
7. In order to protect the right of privacy, no names or specific addresses contained in department records may be used;
8. The Detroit Police department shall be given a credit line for providing data in any report published by the Detroit Police Department and shall review and approve the reports as it pertains to data provided by the department, prior to publication; and
9. Requests to accompany officers on runs or calls, or to spend any time interviewing a number of officers, shall be reviewed individually. Supervisors to whom such requests are made shall bear in mind the severe constraints placed on officers' time.

307.3 - 5 Responsibility for Accuracy, Completeness, and Currency

The Detroit Detention Center (DDC) shall have the sole responsibility to forward correct and accurate arrest data to the Michigan State Police via 10 print fingerprint submission, which is processed through the Live Scan terminals located at the Detroit Detention Center, building 500. Identification shall be responsible for notifying the DDC for any discrepancies found by the Michigan State Police, Technicians from Identification will also notify DDC personnel when a fingerprint is unreadable and the subject needs to be reprinted before the individual is released from custody. It will be the sole responsibility of the DDC to reprint and send legible prints for identifications before the subject is released from custody of the DDC.

This action will prevent the States computer system to cause an untimely delay in positive identification of the subject in custody. Corrections of any discrepancies found relating to the arrest fingerprint submissions will be dealt with in a timely manner to ensure correct and complete data is being forwarded. This will prevent any scenarios that will cause the States Computer system to fail in producing a positive identification on the subject which effects prompt judicial review and the timely manner in which the subject is released.

Checks and balances are needed in order for responsible, accurate, completeness and currency for Computerized Criminal History's. When a fingerprint discrepancy is found by MSP, a notification is made to Identification concerning the issue, if a correction can be made without having the subject in custody reprinted, it will be corrected by Identification personnel. If the subject needs reprinting, notification to the DDC will be made by Identification personnel to have the subject reprinted.

In order for a (CCH) to be complete and accurate a positive identification of an arrested individual has to be made. Several key components must take place before this can occur. First, the arrested subject has to be fingerprinted correctly by a Michigan Department of Corrections Officer. Second, the fingerprints have to be compared by the Michigan State Police Automated Fingerprint Identification System (AFIS) which sends a response back through Talon (LEIN) that the prints have been compared for positive identification of the subject in-custody. If an error occurs and the fingerprint submission is not comparable, a Technician (DPD) or Analyst (MSP) must identify the error and correct it.

Human interaction must take place in order to narrow the five (5) possibilities the computer system (AFIS) gives you. Third, and last but not least, errors that occur when a bad set of fingerprints is submitted will result in untimely delays for positive identification of an arrested subject and cause the States computer system to produce a double State Identification number or (SID) which could result in a subject being released without positive identification being made correctly. Complete and accurate Computerized

307.3 Computerized Criminal History

Criminal History records are most accurate when the proper fingerprinting technique occurs along with correct data being entered on the subject, such as: date of arrest, charge, gender, race, height, approximate weight, hair color and eye color, date of birth, and current address.

There are three (3) sections in the Computerized Criminal History (CCH). The arrest segment of the criminal history is the sole responsibility of the arresting agency and shall be updated by the officer in charge of the case. The prosecutor segment is updated by the prosecutor's office handling the case. The judicial segment is updated by the courts after the case has been adjudicated.

307.3 - 5.1 Access Review and/or Challenge by a Citizen

Any individual about whom criminal history information is maintained and whose identity is satisfactorily verified by fingerprint comparison, shall be entitled to review that information and obtain a copy when necessary for the purpose of challenge or correction. However, the individual's right to access and review shall extend exclusively to computerized Criminal History record information and shall not include intelligence or investigative records.

307.3 - 5.2 Obtaining Computerized Criminal History (CCH) Record for Review

All citizen requests to review *their personal* computerized criminal history records will be handled by the Michigan State Police. Therefore, if a citizen appears at a precinct station or *Records Management* requesting a review of their Computerized Criminal History records, their fingerprints shall be recorded on an applicant fingerprint card and returned to him/her. The requesting individual shall then be instructed to forward the applicant fingerprint card, along with a letter requesting their record, to the Michigan State Police, Records and Identification Division, 7150 Harris, Lansing, Michigan 48913. The Michigan State Police Records and Identification Division will return, by mail the record and fingerprint card to the requesting individual. Any individual wishing to review criminal history record information maintained about him/her by this department shall be directed to appear at *Records Management* between the hours of 8:00 a.m. and 4:00 p.m., Monday through Friday.

307.3 - 5.3 Challenging Computerized Criminal History Information

Any individual who, after reviewing their record, believes that the information is inaccurate or incomplete and wishes to challenge such information, shall be directed to *Records Management* only if this department contributed the information being challenged.

If the information was contributed by this department, the individual challenging such information shall be required to give a correct version of the information and explain why he/she believes his/her version to be correct. *Records Management* shall provide an administrative review and any necessary correction.

307.3 - 6 Logging Computerized Criminal History Requests

The criminal justice information systems rules and regulations require that appropriate records be maintained to facilitate audits of criminal history record information dissemination. Therefore, in compliance with this mandate, all computerized criminal history transactions, whether the response is positive or negative, shall be logged and maintained. With the recent requirement that the terminal operator's name and the name of the person requesting CCH information be included as part of the transaction, all logging of CCH inquiries will now be performed by the computer.

307.3 - 6.1 Audit of Inquiries

To help ensure the integrity of the system, state and federal authorities, as well as Technical Support, will make periodic checks on information requested. The NCIC and LEIN systems will also be identifying each specific agency's terminal location, terminal operator and requestor's name when entering or receiving information from the computerized criminal history records. Furthermore, a record of each transaction will be maintained. It shall be incumbent upon all terminal operators to ensure that CCH inquiries include complete and accurate information.

307.3 - 6.2 State and Federal Authorities

All computerized criminal history inquiries are subject to audit by state and federal authorities as provided under Title 28, Rules and Regulations on Computerized Criminal History Records. Technical Support shall make computerized logs available upon request of Criminal Justice Data Center personnel for audit purposes.

307.3 - 6.3 Technical Support

Technical Support shall generate a monthly computer printout for each terminal, listing all the computerized criminal history inquiries made by that terminal for that period. The listing will be forwarded to the commanding officer at each computer terminal location along with a cover letter. The printout shall provide a means by which command personnel can monitor CCH transactions. Special attention shall be paid to that part of the print out which indicated the name of the person who requested the CCH. Any irregularities in the utilization of CCH information shall be investigated by the command where the inquiry originated. Technical Support will provide technical assistance when necessary.

307.3 - 6.4 Retention of Computerized Logs and Printouts

The computer printouts of CCH transactions distributed monthly by Technical Support will be retained for one (1) year by the receiving commands. It is not necessary to return these printouts to Technical Support. Any questions concerning these printouts shall be directed to Technical Support.

Technical Support shall retain a computer tape log of all CCH computer printouts. Information residing on these tapes will be available upon request to Technical Support.

307.3 - 7 Sanctions for Non-Compliance

Both LEIN and NCIC computerized criminal history records are available to DETECTS users. Inquiry formats and terminal operational instructions are defined in the DETECTS Manual. Summary computerized criminal records will be available by direct computer response.

Members and employees shall bear in mind that his/her right of direct access to computerized criminal history data is restricted to what can reasonably be construed to be related with his/her criminal justice responsibilities. Failure to comply with state and federal regulations, as well as LEIN/NCIC rules may result in suspension or elimination of accessibility to the Computerized Criminal History record, loss of LEIN services and/or fines by the Department of Justice.

307.3 - 8 Computer Terminal Operation

307.3 - 8.1 Authorized Personnel

Authorization to operate equipment and devices of the Detroit Electronic Computer and Teleprocessing System (DETECTS) shall be restricted to personnel who have received proper training and certification in the care, handling, and operation of such equipment. All department members who utilize a computer terminal in the performance of his/her daily duties shall complete the certification of training with the exception of members assigned to Communications *Section*. Certification training is a five (5) day class session held at the Training Center. A schedule of these sessions is disseminated on a semi-annual basis.

Certified terminal operators shall attend a one-day training session for a re-certification at the Training Center on an annual basis. Commanding officers shall designate a supervisor to schedule classes for certified personnel within the command. In cases where attendance would impose an extreme hardship on the terminal operator's command, the commanding officer shall prepare a written explanation. All requests for exemption shall be submitted to the commanding officer of Technology Support through official channels. In no case will any terminal operator be exempted from attending the training class for two (2) consecutive years.

Persons authorized to operate equipment and devices of the DETECTS System shall adhere strictly to all applicable rules and regulations of the Detroit Police Department, the Law Enforcement Information Network (LEIN), the National crime Information Center (NCIC) and the DETECTS Manual.

307.3 - 8.2 Security Access Procedure

The security access procedure is designed to increase accountability through audit procedures, which provide a means of investigating improper uses of the computer

system. In keeping with DETECTS standards, terminal operators shall be required to "sign-on" and "sign-off" when utilizing the computer system. Before performing any transactions, terminal operators shall "sign-on" by entering his/her individual name, pension number, and a personal code (password) into the computer terminal. In order to ensure the integrity of these codes, the individual's personal information will not appear on the terminal screen at any time. Personal codes will *be stored within* the computer and will be known only to the individual terminal operators. Terminal operators shall not reveal his/her personal codes to another person for any reason, nor shall he/she sign-on the computer to allow other persons to utilize the system. Terminal operators shall sign-off the system immediately upon completing a transaction or series of continuous transaction.

If it is determined by the officer in charge that no person assigned to work an inside detail has authorized access to the computer system, the officer in charge shall contact Technical Support - Help Desk. Temporary arrangements will be made to enable a person from within that command, designated by the officer in charge, to have access to the computer system for that particular tour of duty. While so designated, such person shall be subject to the procedures and restrictions as herein provided. Operational instructions for signing on a signing off the terminal are set forth in the DETECTS Manual.

Any computerized information obtained through the DETECTS system or the Mobile Data Terminal (MDT) system is to be used only for official department business. Any irregularity in the utilization of information obtained through the DETECTS system or the MDT system shall be investigated by the command where the inquiry originated.