

Truro Police Department

MANAGEMENT INFORMATION SYSTEMS

Policy Number: ADM-1.09

REFERENCE: Pamet System, TPDM ADM-1.12

Effective Date: June 1, 2000

Revised Date: November 20, 2008

Accreditation Standards: 13.1.1. - 13.2.3. 82.1.1

Mass. Gen. Law

Other:

POLICY:

It is the policy of the Truro Police Department to maintain a management information system in order to provide reliable information to be used in management decision-making.

This is important in predicting workload, determining manpower needs, budget preparation and other resource needs. Access to data contained in the system must be controlled in a manner that will ensure only authorized access. It is also necessary to permit dissemination of public data to interested individuals, in conformance with the standards of the Massachusetts Criminal History Systems Board, and to the extent that the rights of any individual are not infringed. All information will be carefully reviewed prior to dissemination to ensure that it is not restricted.

PROCEDURES:

- 1.** **ADMINISTRATION:** The Information System provides a comprehensive picture of the department's operations at any given point in time, as well as providing information for projecting future trends from current and past data.
 - A.** The Chief of Police is responsible for developing, establishing and maintaining a management information system.
 - B.** Responsibility for recording and/or providing specific types of data is assigned to and/or shared by various Divisions or individuals as follows:
 - 1.** Patrol Division - Calls for service, trespass list, attendance, arrest bookings, stolen property, names, incident report narratives, field interviews, vehicles and tows, abuse restraining orders, summons, subpoenas etc.

2. Administration/Records - Criminal history, firearm permits/licenses, Uniform Crime Report Coding, warrants, motor vehicle citations, and accidents records, statistics, etc.
 - a. Motor vehicle citation shall be kept in the records room, and are available to all officers as needed.
 - b. Citations shall be entered in the central records system (computer system) and accounted for.
 4. Administration/Chief of Police - Training records, personnel, department inventory, geographical data, department policies, general orders, memos, etc.
 5. The Communications Division will be responsible for recording all calls for service, maintaining master cards, recording vehicles and police tows, entering pertinent data in the computer system, and any other recording deemed appropriate. *(Revised August 12, 2003)*
- C. The Responsibility for reviewing, correcting and reporting of collected data is assigned to the Staff Sergeant, Administrative Assistant, and the respective personnel who entered the data.

2. ADMINISTRATIVE REPORTS: Reports reflecting comparative data and trends on activities shall be created annually.

- A. **ANNUAL REPORTS:** The Annual Report shall summarize comparative data and statistics, and account for the activities of this department. NIBRS reports, arrests, trends and other reports required of subordinates may be included if deemed necessary by the Chief of Police.
- B. **DISSEMINATION:** Annual reports shall be disseminated to affected organizational personnel, as well a Town Officials, and the public as directed by the Chief of Police.
- C. **UNIFORM CRIME REPORTS:** The National Incident Based Reporting System (NIBRS) shall be utilized in tracking incidents for reporting purposes. The Administrative Assistant shall be charged with administering these reports. *(Revised August 12, 2003)*

3. RECORDS:

- A. DISPOSITION /DISPOSITION OF CASES:** The Prosecutor/Investigator and the Administrative Assistant are jointly responsible for properly recording all active and final dispositions of cases into the Court Tracking Application. The following procedure shall be followed in the recording of dispositions: *(Revised August 12, 2003)*
1. All final dispositions of court cases shall be recorded on the appropriate case folder.
 2. If the court case was continued to another date, The Prosecutor/Investigator shall make an entry in the defendant's record with the date of continuance, name, docket (case) number, and hearing type, officers needed and any other pertinent data.

The Offender History System serves as a permanent record of the police department and may follow a defendant's criminal history through his career. All personnel are to keep information contained in the Offender History System in utmost confidence. Information contained on master cards are to be divulged only by designated personnel in methods that have been approved by the Truro Police Department. (See TPDM ADM-1.12)

1. An Offender History shall be initiated for the following reasons; when a crime is committed (felony or misdemeanor), when a criminal motor vehicle offense is committed or when a summons is issued from the court for any reason.
2. An Offender History shall contain the following information; name, address, occupation, social security number, alias, place of birth, date of birth, mother, father, height, weight, complexion, color of eyes, color of hair, date of issue, docket number, age, date of offense, offense, arresting officer, date of court appearance, issuing court, final disposition of case, and other relevant data.
3. Offender Histories for adults and juveniles shall be segregated electronically.
4. Upon order of the court, juvenile records shall be expunged in accordance and as directed by the Court. *(Revised November 20, 2008)*.
5. Juvenile records of adult individuals shall only be accessed by authorized personnel. *(Revised November 20, 2008)*.
6. Access to these records shall be on a "need to know" basis.

7. Any records held by the Truro Police will not be released to the public. A law enforcement agency may obtain records if authorized by the Shift Commander on duty. An incident will be made to that affect. All records shall only be released to the public in writing. (see ADM-1.07 Request for Reports for guidance) *(Revised August 12, 2003)*

B. POLICE REPORT FILING SYSTEM: The following procedures shall be adhered to when filing or retrieving reports:

1. All reports shall be written and saved in the in house Pamet PoliceServer computer system, using the assigned incident number generated by the computer. Complete master card information, vehicle information, property information, locations and times of incident, actions and dispositions, and other pertinent data shall be recorded. Police reports shall be finished before the end of a shift. (see TPDM ADM-2.02 for further information)
2. Master card information shall contain the following information; name, address, occupation, social security number, alias, place of birth, date of birth, mother, father, height, weight, complexion, color of eyes, color of hair etc.
3. The printed report shall be transferred to the Staff Sergeant, who is assigned to review reports. If court action is imminent, the report shall be forwarded to the Prosecutor/Investigator. *(Revised August 12, 2003)*
4. The Staff Sergeant will review said report, and forward the report to the Prosecutor/Investigator if needed, who will follow up on the case. The report will then be forwarded to the Administrative Assistant for filing. At anytime during this process, the report may be forwarded to the reporting officer for corrections, additions or further investigations. *(Revised August 12, 2003)*
5. If personnel need to remove a report from the file system for any reason they shall return the report to the Administrative Assistant for filing as soon as possible.

C. All incidents reports, arrests, summons, motor vehicle violations, and various other records are entered into the department computer system and are assigned a unique and sequential incident number. These records may be accessed by departmental personnel from any network computer or terminal, and is available 24 hours a day.

1. Hard copies of all records are maintained in the records room. This cabinet is locked in the absence of the Administrative Assistant.
2. All juvenile hardcopies of reports are stamped JUVENILE on the folder.

D. FINGERPRINT CARDS:

1. Fingerprints shall be taken of all persons arrested, or applicants for employment or licensing purposes.
2. Two cards (one black and one red) shall be taken of all arrests, and employment applicants. One black card shall be sent to the Massachusetts State Police, one red card retained by the Truro Police.
3. Fingerprints of suspects, applicants, and other persons will be maintained in the fingerprint file, located in the Prosecutor/Investigators office. Cards will be maintained in alphabetical order.
4. All officers assigned as photographers and/or evidence officers shall have access to the fingerprint card system. Requests for cards shall be submitted through the Prosecutor/Investigator, any Sergeant or the Lieutenant.
5. Fingerprints shall only be disseminated to legitimate law enforcement agencies for lawful purposes.
6. Juvenile fingerprint cards are stamped JUVENILE and are filed separately in the fingerprint card storage cabinet.
7. If fingerprint cards are removed and subsequently turned over to another department or entity, an incident will be made indicating the officer in charge, the agency and person requesting the cards, the reason, time, date etc. Upon return, another incident will be made indicating that information.

E. PHOTOGRAPHS

1. Photographs will be taken of all arrested persons, job and license applicants. These photographs become a permanent record of the department, and will be taken by the digital camera in the booking area. If in the case of an arrest, a photo will be printed and affixed to the case folder.
2. The Administrative Assistant will process all other photographs.
3. Photographs are stored in the central records system (Image Server) and can be accessed 24 hours a day. Hardcopies are not kept on file.

4. Juvenile photographs, like other photographs of individuals, are stored under their master card in the central computer system. The MasterCard indicates to users the age of the subject prior to photograph retrieval.
5. Booking photo requests from police departments will be made through the officer in charge, the Investigator or the Lieutenant. An incident will be made indicating the officer in charge, the agency and person requesting the cards, the reason, time, date etc. If the booking photo was not a digital image, another incident will be made indicating that return information. Public records request will be made through the Administrative Assistant following the Request for Reports Policy.
(Revised August 12, 2003)

4. EQUIPMENT HARDWARE, SOFTWARE AND SYSTEMS:

- A. Settings on all hardware, including all computers, laptop computers, printers, scanners, and monitors shall not be changed without the authorization of the Chief of Police. Connecting cables shall not be removed and/or reconnected without authorization of the Chief of Police.
- B. **No one may modify software** to computers under control of this department without authorization of the Chief of Police. Installing any outside or other than agency approved software is prohibited without the permission of the Chief of Police. Unlicensed software is prohibited. *(Revised February 6, 2008)*
- C. Using outside or other than agency approved data storage devices in department computers is prohibited without the permission of the Chief of Police. *(Revised February 6, 2008)*

5. PASSWORDS/COMPUTER ACCESS/SECURITY:

- A. Access codes (user names) and the initial users password for the Pamet PoliceServer Computer System including shall be assigned by the Administrative Assistant. Users may not divulge their passwords to anyone without authority of the system manager (A/A). Users shall change the initial password immediately after receiving it. Users may change their password at will. Access codes shall be audited to verify all logins. Logins will be audited annually. Logins no longer needed shall be removed. Passwords are encrypted and are known only to the user. The system manager may change a user's password.
- C. The Administrative Assistant will ensure that records on the department's centralized computer system shall be backed up onto tape daily. These tapes shall be rotated daily including weekends and holidays. The process is automated. *(Revised November 20, 2008)*

- D.** A complete system backup shall be made annually. The back up tape shall be stored and locked by the Chief of Police. *(Revised November 20, 2008).*
- E.** An annual audit of all security codes, passwords and/or access violation, if any, shall be reviewed by the systems manager. This review shall be conducted by the system manager (Administrative Assistant) in the month of June every year. This review shall be noted on the Fiscal Year Calendar of the department.