Waltham Police Department
CHAPTER 13
MANAGEMENT INFORMATION SYSTEMS

General Order Number: GO-03
Effective Date: 01/2009, 05/2014, 4/24/17
Accreditation Standard #'s: 11.4.4, 41.3.7, 82.1.1, 82.1.2, 82.1.4, 82.1.6, 82.1.7, 82.3.4, 82.3.5

POLICY:

It is the policy of the Waltham 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 Systems History 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 Office of Planning and Research 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 Units as follows **[82.3.4]**:

        1. Patrol Division - Calls for service, trespass list, attendance, arrest bookings, stolen property, names, incident report narratives, vehicles and tows.

        2. Records/Community Services Div. - Criminal history, stolen property, firearm permits/licenses, Uniform Crime Report coding, warrants, abuse restraining orders, summons, subpoenas, motor vehicle citations and accidents.

3. Investigation Division - Stolen Property, case narratives, pawnshop activity, domestic violence, juveniles and drug files.

4. Administration - Training records, field interviews, and accidents, evidence, personnel, department inventory, emergency notification list, geographical data, rolodex file and the Waltham Police Department Manuals.

5. The Emergency Telecommunications Division will share responsibilities for recording calls for service, vehicles and police tows, and any other recording deemed appropriate.

c. The Responsibility for reviewing, correcting and reporting of collected data is assigned to the Planning and Research Unit, and the respective units/users that entered the data.

2. **REPORTS:** Reports reflecting comparative data and trends on activities shall be created daily, monthly and annually. **[82.2.4]**

a. The Daily Journal shall summarize department activities during the previous 24 hours and shall be distributed to the Patrol Div., Investigation Div., Report Review Officer, and Planning and Research Unit. The daily journal can be accessed online in our QED system. The journal is printed by the cadet or in the absence of a cadet, the OIC. The Journal is kept in a binder making prior activities readily available. Specific dates can be summarized upon request. **[82.2.4]**

b. The monthly report shall contain information relative to activities of various units for the previous month. This report may also contain year-to-date data, UCR reports, arrests, trends and other monthly reports required of subordinates. The reports shall be prepared by the commanding officer of each division.

c. The Annual Report shall summarize the monthly reports. This report, prepared by the Planning and Research Officer, shall provide comparative data and statistics, and account for the activities of this department.

d. **DISSEMINATION:** Monthly and annual reports shall be disseminated to affected organizational units as directed by the Commanding Officer - Administrative Division. **[82.2.4]**

e. **UNIFORM CRIME REPORTS:** The Uniform Crime Reports (UCR) shall be prepared utilizing the UCR application in the Management Information System and the F.B.I. Uniform Crime Reporting Handbook.

The Planning and Research Officer is responsible for submitting UCR data and correcting any errors found in the report." **[82.1.4]**

3. RECORDS:

a. DISPOSITION SHEETS/DISPOSITION OF CASES [82.2.4]: Records Unit personnel are responsible for properly recording the final dispositions of cases into the Prosecution Management Application. The following procedure shall be followed in the recording of dispositions:

1. All final dispositions of court cases shall be recorded on the appropriate record.

2. If the court case was continued to another date, Records Unit personnel 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.

b. RECORD CARDS/OFFENDER HISTORY APPLICATION: [82.3.5]

The use of Record Cards was discontinued in 1992 when our criminal history records were computerized. These cards are still available for reference in the Records Department.

The Offender History System serves as a permanent record of the police department and may follow a defendant's criminal history through his/her career. Records Unit personnel are to keep information contained in the Offender History System in utmost confidence. Information contained on record cards are to be divulged only by designated personnel in methods that have been approved by the Waltham Police Department.

1. An Offender History shall be initiated for the following reasons; when a crime is committed (felony or misdemeanor), when a party is arrested; when a criminal motor vehicle offense is committed or when a summons is issued from the court for any reason. OBTN (Offender based tracking numbers) are assigned to each individual. **[82.3.5]**

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, and final disposition of case.

3. Offender Histories for adults and juveniles shall be segregated electronically. **[82.1.2-1]**

4. Upon order of the court, the Records Division shall inform the records clerk to expunge (shred) all hard copies of juvenile records. He shall also instruct the Planning & Research Officer (IT) to erase all electronic versions of juvenile records. **[82.1.2-12]**

5. Juvenile Records shall be maintained as such after an individual has become an adult. **[82.1.2-11]**

6. Access to these records shall be on a "need to know" basis. If access is needed, it shall be authorized by Records Unit personnel or in their absence by the Commanding Officer - Platoon on Duty. The Central records division/ Community Services Division is closed after day time hours and all records locked within that office. Three doors enter/exit Community Services, all of which are controlled by FOB access. When open, request for records by agency personnel can be made to the records clerk. **[82.1.1-2A, B], [82.1.2c, d]**. All court and prosecution records are locked in file cabinets within a The Investigations Division, which is limited FOB Access to authorized personnel only. Sexual Assault records, and sex offender records are also locked within a separate filing system within the controlled access Investigations Division. **[82.1.1-2A]**

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

1. The Report Review Officer shall originally file all reports.

2. If a person needs to remove a report for any reason, he shall **NOT** return the report to the file drawer, he shall instead place the report in the basket on top of the file cabinet marked "Reports to Be Filed".

3. The Report Review Officer, or his designee, shall file the reports in the proper place the next working day.

d. All incident reports, arrests, summons, motor vehicle violations and various other records are entered into the department computer system and are assigned a unique and sequential case number. These records may be accessed by department personnel from any network computer or terminal and is available 24 hours a day. **[82.1.1B]**

4. EQUIPMENT HARDWARE, SOFTWARE AND SYSTEMS:

a. Settings on all hardware, including all personal computers, laptop computers, printers, scanners, and monitors shall not be changed without the authorization of the IT. Connecting cables shall not be removed and/or reconnected without authorization of the IT Unit.

b. No one may add or modify software to computers under control of this department without authorization of the IT. No one may introduce outside computer disks into the agency's computer system or at an individual workstation without the authorization of the IT/Supervisor. Only properly licensed software may be used. Pirated or illegally copied software shall not be introduced to any computer.

5. PASSWORD/COMPUTER ACCESS/SECURITY: [82.1.6c, 82.1.7]

a. Access codes (logins) and the initial user's password for the Public Safety Computer System including, mobile systems, shall be assigned by the Planning and Research Unit. Users may not divulge their passwords to anyone without authority of the system manager. Users shall change the initial password immediately after receiving it. Passwords shall age and expire between 150 and 180 days. 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**. [82.1.6]** Passwords are encrypted and are known only to the user. The system manager may change a user's password.

b. Access codes (logins and the initial user's password for the City of Waltham computer network (WALNET) is provided by Network Engineering who manages WALNET. This network provides electronic mail, access to the internet and access to shared resources on the network **[82.1.7B]**.

c. Software and hardware have been installed to prevent unauthorized network access from outside the city's network (WALNET).

d. The records on the department's centralized computer system (H Drive and QED system) are all electronically backed up daily. There are three central backup server rooms at different offsite locations; one is located at City Hall, one at the 911 Dispatch Center and one at the Government Center. **[82.1.6]**

e. Release of any computer records, including digital photos, criminal history, arrest/other reports, etc. are to follow the same protocol for releasing records out of the Community Services Division. **[82.1.7C]**

6. CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES:

The department's Criminal Intelligence System shall be operated in compliance with 28 C.F.R. Part 23 as it pertains to operating principles.

28 C.F.R. Section 23.20 Operating Principles:

a. A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

b. A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

c. Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis [[Page 355]] to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

d. A project shall not include in any criminal intelligence system information that has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a property trained participating agency which is subject to routine inspection and audit procedures established by the project.

e. A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

f. Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

g. Paragraph (f) (1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

h. A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

1. Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

2. The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

3. The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

4. The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

5. The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

6. A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements. [Page 356]

i. All projects shall adopt procedures to assure that all information that is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information that is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes that involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

j. If funds awarded under the Act are used to support the operation of an intelligence system, then:

1. No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to ensure that it is accessible only to authorized system users; and

2. A project shall undertake no major modifications to system design without prior grantor agency approval. (ii) [Reserved]

3. A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

4. A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other

device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C.2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

5. A project shall make assurance that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

6. A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

k. A participating agency of an inter-jurisdictional intelligence system must maintain in its agency files information that documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting the system submissions must be made available for reasonable audit and inspection in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

l. The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

7. POLICY FOR MOBILE DATA COMPUTERS [41.3.7-1B]:

a. System Access & Utilization

b. All officers wishing to utilize any computer shall receive a basic training class and/or instruction from the Planning & Research Office or an authorized trainer. Officers will be assigned a user account and password and are not to use any computer system without having been assigned such an account. The user account information shall not be shared with any other individual and no member may use the password of another.

c. The mobile data computer system is the preferred method of communication for special assignments, sensitive calls and other general unit-to-unit communication. Mobile communications shall conform to FCC guidelines regarding radio transmissions and shall not contain improper language or subject matter.

d. All motor vehicle stops, field interviews, etc., shall be radioed into communications despite the fact that all CJIS information may be obtained through a mobile computer.

e. The mobile computer is not to be utilized by an officer operating a vehicle while the vehicle is in motion as this may divert the officer's attention from the safe operation of the vehicle.

f. No software, other than **CJIS Mobile,** is to be used or installed on any mobile computer without express permission of the Planning & Research Office.

8. EQUIPMENT:

a. At the start of each shift, officers shall check the mobile data computer while completing the regular vehicle equipment checks. Officers shall log onto the assigned mobile computer and remain active on the system for the duration of the tour. Any problems and/or damage to any mobile computer shall be immediately reported to the Officer in Charge. The Shift Commander will be responsible to notify the System Administrator.

b. NO food, beverages or any other substance that might cause damage will be placed on or near a mobile computer.

c. Officers shall be responsible for any damage to mobile computers during their tour.

d. The Operating temperature of a mobile computer is normally between 50- and 85-degrees Fahrenheit. If the police vehicle has not been used during the previous tour in cold weather, the vehicle should be run for at least twenty (20) minutes with the heater running before attempting to turn on the computer.

e. If the mobile computer is not functioning:

1. Check to see that it is turned on.

2. Visually check to see that cables in the rear of the computer are secure.

3. Check the radio and the modem in the trunk to see if they have power.

4. Check with dispatch to determine if other units are logged in or having problems.

5. Notify the Officer in Charge of the problem and submit a report to Planning and Research.

f. Officers must logoff at the end of their tour so that they are not responsible for further transactions from that mobile unit. The computer shall be shut down at the end of their tour. If the patrol unit will be used on the next shift, the computer may be left on for the next officer.

9. INFORMATION ACCESS:

a. The mobile data computer system's database access (NCIC/CJIS/RMV) is for inquiry only. No entries can be made. Federal Law, Title 28 as well as Massachusetts Statutes regulate access and dissemination of NCIC/CJIS/RMV. All inquiries made using a mobile computer are subject to these guidelines.

b. No information received through any State or National computer database will be released to any unauthorized individual or civilian.

c. Requests for police reports by the general public are directed to the Community Services Division. An attorney may request record/reports in person only and must have a singed release from his/her client. Reports will only be released when the report states "Authorized for Release" on top. This indicates that the report has already been reviewed and approved by the supervisor of records and/or Investigation Division. Only those individuals named/involved in the report shall be given a copy of this report. All requests go through the Community Services/Records Division during open hours and if charged, are recorded on the payment log. **[82.1.1-2D, E]**

d. Requests for police reports from other police agencies will also be directed to Community Services during business hours. After hours, police reports can be released upon request to other police agencies with the authorization of the Officer in Charge, Patrol Division. **[82.1.1-2C]**

10. AUDIBLE ALARMS: The current 2009 packet cluster system no longer has audible alarms, warning of warrant or any other "hits".

11. MOTOR VEHICLE STOPS, DRIVING WHILE SUSPENDED VIOLATIONS & "HIT" RESPONSE:

a. For officer safety reasons, the vehicle's registration number should be entered for inquiry before exiting the patrol vehicle.

b. Officers are encouraged to query as many registration numbers as possible during a tour of duty. Probable cause to stop shall be established prior to initiating a stop.

c. A police officer can run a motor vehicle query without any prior suspicion of wrongdoing.

d. As a result of information received, the officer may make a valid stop for problems related to the vehicle itself and/or the owner's driver's license.

e. The following must precede stops based upon license plate inquiries that indicate the registered owner's license is suspended:

1. After receiving the suspension information, the officer must attempt to verify that the driver of the vehicle to be stopped generally matches the sex/age description of the registered owner listed on the mobile computer screen.

2. When the information reveals a problem with the vehicle itself, a valid stop is proper without any further corroboration.

3. In the event an inquiry results in a NCIC/CJIS "HIT" response, all online system users with automatically be notified via alarm. All "HITS" shall be confirmed through the communications center prior to taking action base solely upon this response.

12. **DATA STORAGE:** All communications and queries shall be recorded and archived at the base station located in the communications center. A System Administrator may conduct system audits as necessary. **[82.1.6-3]** Back up files are conducted daily on the server. **[82.1.6-2, 4]**

13. **AUTHORITY/PERMISSIONS:** In order to protect the Department computer system, Employees shall not install unauthorized or unlicensed software on any Department computer. **[11.5.1-1a], [41.3.7-3B]** No unauthorized programs or material may be transferred from floppies, CD's DVD's, thumb drives, or from online sources to any Department computer. **[11.5.1-1b, c],** Employees shall not manipulate or alter current software running on agency-owned mobile, desktop or handheld computers. **[41.3.7-3B, C]**