


Atlanta Police Department Policy Manual		Standard Operating Procedure
Effective Date May 5, 2021		APD.SOP.3062 In-Vehicle Computers
Applicable To: All sworn employees		Review Due: 2025
Approval Authority: Chief Rodney Bryant		
Signature: Signed by RB		Date Signed: 5/4/2021

Table of Content

1. PURPOSE	1	4.6 Security of Laptops	6
2. POLICY	1	4.7 Laptop Computer Mobile Data function	6
3. RESPONSIBILITIES	1	4.8 Restrictions for Laptop/Vehicles	7
4. ACTION	2	4.9 Training	7
4.1 Dispatching and Communications	2	5. DEFINITIONS	7
4.2 Supervisors' Responsibilities at Start of Watch	3	6. CANCELLATIONS	8
4.3 Officers' Responsibilities at Start of Watch	3	7. REFERENCES	8
4.4 Incident Report Writing Process	4	8. SIGNIFICANT CHANGES	8
4.5 Report Approval Process	5		

1. PURPOSE

To establish procedures for the usage of mobile laptop computers (also known as Mobile Data Terminal (MDT)) used in patrol vehicles and other Department vehicles; including capabilities, access, security issues, and restrictions on the use of vehicles equipped with mounted laptop mobile data terminals.

2. POLICY

It is the policy of the Atlanta Police Department to use in-vehicle computers for official use only, properly handle and safeguard computer data, and maintain the equipment in good working order.

3. RESPONSIBILITIES

- 3.1 Section commanders shall implement this directive in their commands. Section commanders shall ensure strict accountability of laptops assigned to their sections and provide secure storage for laptop computers that are not in use.
- 3.2 The Chief Administrative Officer shall coordinate with Atlanta Information Management (AIM) for the timely updating of the software, hardware, and other data on the laptops as necessary. The Central Records Unit shall manage drop down and pick lists within the records management systems (RMS).
- 3.3 Supervisors shall monitor and ensure the correct use of the laptops.
- 3.4 The Electronic Maintenance Unit (EMU) shall maintain and control in-vehicle laptop computer hardware.



ATLANTA POLICE DEPARTMENT POLICY MANUAL

APD.SOP.3062 In-Vehicle Computers



- 3.5 AIM shall maintain the laptop computer software.
- 3.6 Employees shall use and safeguard the laptop computers properly and in accordance with departmental training. They shall adhere to GCIC and department regulations, ensuring that the information obtained from laptops are used for official business only. (CALEA 6th ed. Standard 41.3.7a-e)
4. ACTION
- 4.1 Dispatching and Communications
- 4.1.1 Personnel shall not use "silent dispatching" or "self-initiating" MDT features except as specified in Section 4.1.4. The officer shall receive a voice message from a dispatcher and shall respond by voice. The MDT shall provide additional (non-voice) information as needed.
- 4.1.2 If the officer gets a "hit" from GCIC via the MDT, verification as required by APD.SOP.3110, "GCIC and NCIC Information" shall be completed.
- 4.1.3 Critical requests from officers shall not be made via MDT, such as a request for a fire/EMS response or a request for backup units.
- 4.1.4 Officers shall only use the computer-aided dispatch (CAD) "self-initiate" dispatch option on the following calls:
1. Direct Patrols and Drop-ins.
 2. Warrants.
 3. Extra Jobs.
 4. Help calls (as additional responding units).
 5. "G" calls to include 19G, 11G and 16G; or
 6. Low priority traffic stops.
- 4.1.5 Officers utilizing self-initiation for traffic stops shall verbalize on radio after one minute if they have not been acknowledged by a dispatcher.
1. Tag information shall be entered into MDT prior to initiating the stop.
 2. Vehicle information to include color, make, model and occupant descriptions shall be entered into the comment section.
- 4.1.6 Officers utilizing self-initiation for calls for service other than traffic stops shall:
1. Create an incident in CAD using the MDT prior to self-initiating.
 2. Create a separate incident using the MDT for any subsequent incidents that occur.
 3. Clear incidents with the correct disposition code (units shall only be allowed to hold themselves out on up to two incidents at a time).



ATLANTA POLICE DEPARTMENT POLICY MANUAL

APD.SOP.3062 In-Vehicle Computers



- 4.1.7 Dispatch may utilize “silent dispatch” on Priority 3 and 4 calls for service.
1. On “silent dispatch” calls, dispatchers shall assign and place the officer on the call via CAD but will NOT verbally raise the officer and give the call out over radio.
 2. Domestic and Suspicious Person calls shall only be dispatched verbally over the radio. The dispatching of these calls by “silent dispatch” is strictly prohibited.
 3. The officer shall acknowledge and place themselves en route to the call via the MDT.
 4. If the officer does not acknowledge the silent dispatch, the dispatcher shall verbally raise the officer over the radio to verify they received the call.
- 4.1.8 Officers shall only clear themselves from calls that are self-initiated or received by silent dispatch using their MDT. All calls that are verbally dispatched and any use of force calls must be verbally cleared over the radio prior to the unit clearing themselves from the call on the MDT.
- 4.2 Supervisors' Responsibilities at Start of Watch
(CALEA 6th ed. Standard 41.3.7e)
- 4.2.1 After roll call, the watch commander or his or her designee shall transmit via facsimile to Communications a daily Roll Call Sheet and/or assignment sheet.
- 4.2.2 Each supervisor shall verify that all officers on duty have notified radio that they are in-service (Code 7) and that they are entered into the CAD system, prior to starting their tour of duty, by their 4-digit identification number.
- 4.2.3 After notification of the officers that will be in service, the dispatcher shall notify the field supervisor after five minutes of officers that have not signed on.
- 4.3 Officers' Responsibilities at Start of Watch
- 4.3.1 The officer shall inspect the MDT and mount at the beginning of the watch. The officer shall document this inspection on the back of the Daily Activity Sheet (Form APD 607) along with the vehicle inspection.
- 4.3.2 If the MDT or equipment are damaged, missing, or inoperable, the officer shall notify a supervisor immediately and complete a report.
1. If the laptop is damaged or inoperable, at the first opportunity, the officer must transport the laptop to the EMU (404-658-6868) at 180 Peachtree Street, 5th Floor EMU, Atlanta, Georgia, 30303; Monday through Friday, between 0800-1600 hours.
 2. If a spare laptop is available at the EMU the officer shall sign it out.
- 4.3.3 After officers are cleared from roll call, they shall immediately begin their tour of duty by advising Communications via radio that they are in-service (Code 7).
1. The officer shall provide Communications with their unique 4-digit ID and assignment.
 2. After advising Communications, the officer shall sign on to the CAD system via the mounted MDT, with his or her assignment, unique I.D., vehicle number and password. If a second



ATLANTA POLICE DEPARTMENT POLICY MANUAL

APD.SOP.3062 In-Vehicle Computers



officer is assigned to the car, his or her 4-digit number should also be entered but not their password.

- 4.3.4 All employees shall operate in-vehicle computers and all components, including air cards (if installed), batteries and other accessories, in the appropriate manner.
- 4.3.5 When exiting the vehicle, officers shall take care not to use the air card as leverage to help them exit the vehicle as this can damage the air card as well as the computer.
- 4.3.6 Officers shall not remove the air card for any reason. If a problem with the air card occurs, the officer shall bring the air card and laptop to EMU.
- 4.3.7 Should the air card become dislodged for any reason, the officer shall make sure the air card is aligned properly with the slot in the in-vehicle computer before inserting it; this shall prevent damage to the equipment.
- 4.3.8 Do not use force to reinsert the air card. With gentle pressure, insert the air card into the receiving slot. If the air card does not slide smoothly or fails to lock into place, stop immediately and take the in-vehicle computer to EMU for air card reinstallation.
- 4.3.9 Officers shall not use the air card as an armrest.
- 4.3.10 Officers shall not remove the in-vehicle computer battery for any reason.
- 4.4 Incident Report Writing Process
 - 4.4.1 Writing Reports
(CALEA 6th ed. Standard 82.2.1d-e)
 - 1. Officers shall use the MDT, whenever they are available in a vehicle, to write incident and accident reports. Officers shall follow the procedures taught in training and contained within the records management systems. When a laptop is not available, the officer shall use the designated precinct desktop computer. If both the laptop and desktop computers are inoperable or unavailable, with a supervisor's approval an officer can use the paper forms as outlined in APD.SOP.3060, "Report Writing."
 - 2. If the officer is unable to complete a report immediately, he or she can save their progress. Generally, officers should complete reports before pulling back in service. All reports must be completed and saved as soon as possible. Unless otherwise approved by the officer's immediate supervisor, all reports must be completed and submitted before the end of the officer's tour of duty.
 - 3. When the officer has completed the report, he or she shall authenticate it in the prescribed manner (electronic signature) and transmit the master report forward for review by a supervisor. No one can alter the report except the submitting officer.
 - 4. When the watch is called, if the officer has any reports to complete, he or she shall complete them at the precinct.
 - 5. Supervisors and officers shall check the RMS inbox regularly during the watch for returned or incomplete reports. (CALEA 6th ed. Standard 41.3.7e)



ATLANTA POLICE DEPARTMENT POLICY MANUAL

APD.SOP.3062 In-Vehicle Computers



6. When multiple officers are writing reports for the same incident or accident, only the reporting officer shall write the original report. All other officers shall write supplements as outlined in APD.SOP.3060, "Report Writing."

4.5 Report Approval Process

4.5.1 Priority Incident Reports

1. For purposes of forwarding an incident report from the laptops to Central Records, a priority report is a report involving a stolen vehicle ~~or~~ a missing person, or the theft of an officer's weapon during an incident.
2. Officers shall notify their supervisor of the priority report via radio or unit-to-unit messaging upon signing off on the report.
 - a. Supervisors shall review, authenticate, and sign off on priority reports without unnecessary delay.
 - b. The reporting officer shall immediately notify the GCIC/Central Records Unit (404-546-5344) via telephone and inform them that a priority report has been completed. The officer shall give the Central Records employee the case number for the report so it can be located on the RMS to confirm that the information for GCIC entry is complete.
 - c. The officer shall include the name of the GCIC employee they spoke with and provided information to in the narrative of their priority report, including the time of the telephone call.
 - d. If the call is deemed serious enough that the supervisor believes any additional time lag for the entry into the GCIC system could jeopardize life, then the supervisor can directly request to the Central Records employee that the entry be made before the police report is completed. The incident report should be completed as soon as possible after the entry is made to ensure GCIC standards are being followed.

4.5.2 Non-Priority Incident Reports

1. Supervisors shall review incident and accident reports either from the supervisor's MDT or a precinct desktop computer. Supervisors should review reports at least every two hours during their watch. They shall approve all reports before the end of their tour of duty.
2. If reports are correct and complete, the supervisors shall authenticate (electronic signature) them.
3. Supervisors shall electronically return rejected reports to the officer and document the additional information needed for the completion of the report in the "reject notes" section of the RMS.
4. The Central Records Unit shall receive, review, and classify incident reports after the officer's supervisor has approved them.
 - a. If the report is rejected, the Central Records Unit shall use the "reject notes" section to indicate what problems must be fixed and electronically reject the report to the officer's mailbox.



ATLANTA POLICE DEPARTMENT POLICY MANUAL

APD.SOP.3062 In-Vehicle Computers



- b. The supervisor on duty when the officer submits the corrected report is responsible for the approval of the report. The original supervisor who signed off on the report previously is not responsible for the approval if he or she is not on duty at the time of the officer's re-submission of the report.
 - c. Central Records' authentication is the final approval. Once the report receives final approval, the report is locked and is no longer able to be edited.
- 4.5.3 At the end of each watch, all officers shall manually purge all reports from the MDT's hard drive by logging out of RMS and deleting/closing any report notes on other software.
- 4.6 Security of Laptops
 - 4.6.1 Only supervisors and designated EMU personnel and their designee(s) shall have a master key to the MDT mounts.
 - 4.6.2 Section commanders, or a designee, shall issue master keys to the supervisors in the section and shall collect them when supervisors are transferred out. Additional keys shall be kept secured by the section commander.
 - 4.6.3, When necessary, the supervisor or EMU is responsible for the removal of the laptop from the mount.
 - 4.6.4 Laptops should be removed and secured at the work site when vehicles are taken to the maintenance shop. With supervisor permission, officers may remove the laptops from the mounts when they are turning in a car for maintenance, and it would be impractical to drive back to the work site prior to putting the vehicle in for maintenance.
 - 4.6. 5 The laptop shall be locked and secured when it is mounted within the vehicle.
- 4.7 Laptop Computer Mobile Data function
 - 4.7.1 The Mobile Data -Computer System is a high-speed two-way data communications network between a land-based computer system and a keyboard/display unit in a department vehicle. Officers shall use the system ONLY FOR OFFICIAL DEPARTMENT BUSINESS.
 - 4.7.2 Major Features of the Mobile Data Function
(CALEA 6th ed. Standard 81.2.8)
 - 1. An officer in the field can inquire directly into automated files or computer systems at the local and state levels, and even up to the computerized National Crime Information Center (NCIC).
 - 2. An officer can receive the following information without going through a dispatcher:
 - a. Tag check.
 - b. Vehicle identification number check.
 - c. Driver's license check.
 - d. Wanted or missing person check.



ATLANTA POLICE DEPARTMENT POLICY MANUAL

APD.SOP.3062 In-Vehicle Computers



- e. Weapons check.
- f. Zone or unit activity status; and
- g. Premise history checks.

4.8 Restrictions for Laptop/Vehicles

- 4.8.1 Other than authorized AIM personnel, employees shall not install, delete, or modify any software and shall not alter computer configurations in anyway. (CALEA 6th ed. Standard 41.3.7c-d)
- 4.8.2 Officers must sign off from the MDT at the end of the tour of duty. This is critical to protect the officer's computer I.D. password. Prior to signing off, the officer shall review and clear all queries, checks and messages that have been generated or stored during the watch.
- 4.8.3 To clean the laptop screen and keyboard, use only the cleaner designated by AIM. Keep all liquids away from the laptop. If spills occur, immediately power down the MDT and clean all surfaces. The MDT should be taken to the EMU for a thorough cleaning.
- 4.8.4 Do not use sharp or hard objects on the MDT's touch screen, including ink pens. Only use fingertips or a computer touch screen stylus.
- 4.8.5 Officers are prohibited from using patrol vehicles to give other vehicles (including patrol vehicles) a "jump start," as this may damage the radio or laptop.
- 4.8.6 Unit-to-unit transmissions are for official business only. Officers shall not transmit any improper messages over the MDT.
- 4.8.7 Officers are prohibited from removing the air card from the lap top computers. Only designated EMU personnel shall remove the air card from the laptop computers.
- 4.8.8 Officers shall not physically alter or attempt to repair the in-vehicle laptop computers, including, but not limited to the mounts and docking stations. All inoperable laptop computers and/or associated equipment shall be taken to the EMU at 315 Chester Ave., Atlanta, Georgia, 30316; Monday through Friday, between 0800-1600 hours for repairs.

4.9 Training

- 4.9.1 The system is designed to operate on a simple, highly automated basis. However, no officer shall operate a laptop without a prior training session.

5. DEFINITIONS

- 5.1 Authentication: A keyboard "signature" confirmed by the user's I.D and password.
- 5.2 CAD (computer-aided dispatch): A program for dispatching resources for emergency services.
- 5.2 CICA number: Complaint, incident, case, and arrest number.
- 5.3 Laptop: A full featured portable computer.



ATLANTA POLICE DEPARTMENT POLICY MANUAL

APD.SOP.3062 In-Vehicle Computers



- 5.4 Mount: The support mechanism/docking station which is utilized for securing and supplying external power and data connections to a laptop computer in a motor vehicle.
- 5.5 Priority report is a report involving a stolen vehicle or a missing person.
- 5.6 RMS (records management system): A program for writing incident and accident reports.
- 5.7 Self-Initiating: The unit holds himself/herself out on an incident via MDT.
- 5.8 Sign Off Screen: The screen for supervisory and Central Records approval of incident and accident reports.
- 5.9 Silent Dispatching: Sending an officer on a call for service by sending a text or data message without audible transmission.
- 5.10 Air card: a device which allows wireless access to the City of Atlanta network when inserted into a slot in an in-vehicle computer.
6. CANCELLATIONS
- APD.SOP. 3062 "In-Vehicle Computers", effective March 15, 2018
7. REFERENCES
- APD.SOP.3060, "Report Writing"
APD.SOP.3110, "GCIC and NCIC Information"
- Commission on Accreditation for Law Enforcement Agencies (CALEA) 6th ed. Standards;
41.3.7a-e, 81.2.8 and 82.2.1d-e.
- Form APD 607 "Daily Activity Sheet"
8. SIGNIFICANT CHANGES
- 8.1 References to PSSI, ICIS and Northrup Grumman removed from policy as a result of conversion to new records management system. Sections 4.4 and 4.5 verbiage updated to reflect new processes for new records management system.
- 8.2 Section 4.1.1 amended, and Sections 4.1.3 to 4.1.8 added to allow for silent-dispatching and self-dispatching under limited circumstances.
- 8.3 Section 4.2.3 added.
- 8.4 Section 4.3.3(2) amended to add vehicle number.
- 8.5 Section 4.5.1 amended to add the theft of an officer's weapon.
- 8.6 Section 4.5.1(2)(b) amended to require officer to provide a case number to Central Records employee.
- 8.7 Section 4.5.1(2)(d) added.