



Florida Fish and Wildlife Conservation Commission
Division of Law Enforcement

DIVISION COMPUTER EQUIPMENT AND USE

GENERAL ORDER	EFFECTIVE DATE	RESCINDS/AMENDS	Applicability
53	January 11, 2017	November 17, 2010	All Members

References

FWC IMPP 3.2, 3.3, 3.4, 3.7 AND 3.8
CFA 32.01

1 POLICY

- A** It is the policy of the FWC Division of Law Enforcement to increase the efficiency and effectiveness of its members through the deployment and use of available technology, including, but not limited to, desktop computers, laptop computers, tablets and associated technology.
- B** It is the policy of the FWC Division of Law Enforcement to establish guidelines and regulations ensuring the safe use of laptops, tablets, and/or any other Division computer equipment by its members.
- C** It is the policy of the FWC Division of Law Enforcement that all members utilizing the MCT and FCIC/NCIC services shall attend Division-approved laptop computer training and successfully complete the CJIS Certification Class prior to assignment and issuance of an MCT.
- D Definitions**
 - (1) Mobile Computer Terminal (MCT)** - Any computer including, but not limited to, desktops, laptops, and tablets that provides for dispatching, car-to-car communications, criminal justice database inquiries and completion of required Division reports and forms.
 - (2) AVL** – Functionality of MCT that shows the location of all MCTs that are logged on with a valid latitude/longitude.
 - (3) CAD** – Computer Aided Dispatch Software provided by CTS America.
 - (4) Self-Dispatch** - Functionality of the MCT that allows the user to perform functions similar to Duty Officers in the CAD System.

2 RESPONSIBILITIES

- A** All members are responsible for being familiar with and adhering to all FWC Internal Management Policies and Procedures (IMPP) as they relate to the use of agency-issued and managed computer equipment, including, but not limited to IMPP 3.2 *Remote Access Policy*, IMPP 3.3 *Password Policy*, IMPP 3.4 *Wireless Communication Policy*, IMPP 3.7 *Information Technology Resource Usage Policy*, and IMPP 3.8 *Computer Security Incident Response and Reporting*.
- B** All members are responsible to use every precaution to safeguard equipment against damage.
- C** All members are responsible to use every precaution to safeguard equipment when the equipment is not in their immediate possession.

3 PROCEDURES

A Assignment, Security, and Storage of Equipment

- (1) Assignment of Equipment
 - (a) Computers shall be issued in accordance with the Commission's established property control procedures.
 - (b) Computer installation in vehicles shall be done in a manner that does not interfere with any occupant restraint devices or occupant safety features (air bags and seatbelts).
 - (c) Members are responsible for the care and security of each piece of equipment assigned to them or to their assigned vehicle/vessel.
- (2) End-of-Shift Removal and Storage of Equipment
 - (a) Following their shift, if the member's vehicle will be secured in a locked garage, all computer equipment may remain in the vehicle.
 - (b) If a member's vehicle will not be secured in a locked garage, the computer shall be removed from the vehicle and stored in the member's residence or office.
 - (c) Computer equipment shall not be left in Commission vessels, ATVs, Buggies or other off-road equipment. The computer may be left on Off-Shore Patrol Vessels as long as the equipment is secured in the wheel house or cabin area.
 - (d) Due to the sensitivity of the equipment to temperature extremes, computer equipment is not to be stored in the trunk of a vehicle, except to be secured in a trunk for short periods of time to ensure security of the equipment. In these instances, the member shall power down the unit prior to placing it in the trunk and remove it as soon as feasible to avoid equipment damage.
- (3) When members assigned to the patrol function are on-duty, the computer shall be securely mounted and locked in the available docking device with the docking key removed. Other members shall have the computer securely mounted and locked in the docking device, unless doing so may not be in the best interest of the member's current assignment (i.e. undercover work, etc.).
 - (a) If there is not an available docking device the member shall take any necessary steps to ensure the computer is protected from damage while driving (e.g. sliding off of seat).
- (4) Unattended Vehicles
 - (a) Vehicles shall be locked when left unattended.
 - (b) Members shall, if necessary, remove the computer from the vehicle.
 - (c) The computer shall not be stored in any location that exposes the computer to extreme heat or cold.
 - (d) Members are required to lock the computer screen if they leave the computer unattended for any period of time.
 - (e) Employees shall log off and power off the computer if it is to be left unattended, for an extended amount of time.
- (5) Unattended Vessels
 - (a) Computers shall not be left unattended in vessels for extended periods of time. The laptop may briefly be left unattended if locked in the docking device.
 - (b) Members are required to lock the computer screen if they leave the computer unattended for any period of time.
 - (c) If it becomes necessary to leave a computer on an unattended vessel, the member shall

securely lock the computer in an appropriate storage area.

(6) Unattended Off-Road Equipment

- (a)** Computers shall not routinely be left unattended in off-road equipment.
- (b)** Members are required to lock the computer screen if they leave the computer unattended for any period of time.
- (c)** If it becomes necessary to leave a computer in off-road equipment, the member shall take any appropriate steps to secure the computer against loss.

(7) Stolen computer

- (a)** The local law enforcement agency having jurisdiction shall be immediately notified when a computer is stolen.
- (b)** The member's immediate supervisor shall also be notified and appropriate chain of command shall be notified so that the Commission's Office of Information Technology (OIT) staff can take necessary precautions to ensure that the FWC Network cannot be accessed by or through the stolen computer.
- (c)** Members shall be held responsible for any stolen or missing item if the vehicle is left unlocked when unattended or when member failed to store the equipment securely on a vessel or off-road equipment.
- (d)** Stolen equipment requires the completion of an Incident Summary Report by sworn members, or the completion of a statement using the Division's memorandum format (FWC/DLE-521) by non-sworn members detailing the particulars of the loss.
- (e)** In addition to the Incident Summary Report or Division Memorandum the member must complete the Computer Security Incident Report on the OIT Share Point Site for all stolen or missing computers.

B Restrictions regarding FCIC/NCIC Access

(1) Members shall:

- (a)** Restrict dissemination of information received through FCIC to authorized criminal justice persons only.
- (b)** Perform transactions for criminal justice purposes only.

(2) Members shall not:

- (a)** Access criminal history files except as provided for by law and rule.
- (b)** Access database records for any reason other than legitimate law enforcement purposes.
- (c)** Permit use of the computer by any individual who is not certified for FCIC access.

C Authorized/ Unauthorized Use

- (1)** Use of the computer is restricted to official Commission and Division business. Computer files, including e-mail messaging and FCIC/NCIC inquiries are subject to review.
- (2)** Use of the computer by anyone other than authorized Division employees requires authorization from the Director, Office of Information Technology.
- (3)** Members are responsible for ensuring the security of the computer against unauthorized use.
 - (a)** Members are required to lock the computer if they leave the computer unattended for any period of time. If the member stays within eyesight of the computer, they are not required to lock the computer. Examples for those situations are standing in hallway outside of office, traffic stops, user checks close to the vehicle, etc.
 - (b)** If it is believed that unauthorized access has occurred, the member shall immediately notify

a supervisor.

- (4) Inappropriate or unauthorized use of the computer may subject the employee to disciplinary action.
- (5) Members shall not use any other member's login name and/or password to log onto a computer.

D Software Restrictions

- (1) Members shall abide by any and all FWC Policies regarding agency computers and software in regards to their assigned computer.
- (2) If a member wants additional software loaded onto the computer, they must submit a written request through the chain of command to the Fleet and Technical Services Section. If the Fleet and Technical Services Section determines that the requested software is appropriate, they shall forward the request to the Director, Office of Information Technology. Only software that is business related shall be approved. Screen savers, wallpapers, games and other non-business-related software are not to be loaded onto computers (this does not include software that is loaded onto the laptop by the Office of Information Technology).
- (3) Any unauthorized software found on FWC computers during maintenance work, upgrades or inspections shall be removed and the member may be subject to disciplinary action.
- (4) Members shall not disable or shut off any software that is loaded on the computer, including, but not limited to, anti-virus programs, AVL, SMARTMCT, etc.

E Computer Operations While on Patrol

- (1) The computer shall be turned on and logged on to MCT at all times that a sworn member is operating their vehicle.
 - (a) If a member is en-route between their residence and their regularly assigned duty station other than a patrol assignment, the member may leave their computer safely stored at the facility to which they are regularly assigned. This includes, but is not limited to, assignments at Regional Offices, Field Offices, the Academy, Aviation Hangars, and GHQ.
 1. While in travel status, members holding the position of Major or above shall not be required to turn the laptop on as described in E (1).
 - (b) If a member is on an investigative assignment or a special assignment, e.g. Resource Protection Service, joint details with other agencies, etc., where it is not practical to have the laptop visible in the vehicle or vessel, the member is not required to turn the computer on as described in E (1). However, the computer should be carried in the vehicle even if not intended to be used by the member during the assignment.
 - (c) Members should have written (email is sufficient) approval from at least a Captain within their chain of command for the situations described in E (1) (a) or (b).
- (2) Members shall take care when operating a computer while driving. Simple inquiries and viewing the nature of an in-coming message may be performed while driving. Message response and complex or multiple inquiries are not to be conducted while driving.
- (3) Foods and beverages are not to be placed on the computer. Care is to be taken to ensure no food, beverage, or other substances are dropped or spilled on any part of the computer.
- (4) Only members with current FCIC/NCIC certification are permitted to initiate inquiries into criminal justice databases.

F Self-Dispatch

- (1) The FWC Division of Law Enforcement shall leverage existing technology in the MCT to use the self-dispatch functionality.
- (2) Self-dispatch shall not replace the use of the radio for the transmission of urgent or emergency

traffic as defined in General Order 26.

- (3) The main goal of self-dispatch is to move routine radio traffic off the radio system so that emergency traffic will not be impeded.
- (4) Status checks (10-13) shall be conducted using the radio.
- (5) The current instructions for self-dispatch use will be maintained on the Mobile Computer Share Point Site located at: <http://portal2.fwc.state.fl.us/sites/le/computer/SitePages/Home.aspx>
- (6) Member Responsibilities
 - (a) Sworn members are responsible for ensuring that their MCTs and AVLs are working properly while using self-dispatch. If the MCT or AVL stops working, they must switch to using the radio for all communications with dispatch.
 - (b) Sworn members shall use self-dispatch whenever possible to replace routine radio traffic.
 - (c) Sworn members shall confirm that any commands they enter are accepted by the system as indicated by the pop-up above the "CAD STATUS", in the lower right hand corner of the screen.
 - (d) Sworn members shall ensure that all required information they enter is correct.
 - (e) Sworn members shall advise dispatch via radio as their zones change during their shifts.
 - (f) Duty Officers shall monitor the Unit Status screen, Active Calls screen, and map to be aware of changes in officer status and created calls.
 - (g) Duty Officers shall ensure all incidents are validated whenever possible.
 - (h) Field Supervisors shall monitor radio traffic and CAD to ensure that sworn members are using self-dispatch appropriately.
 - (i) Duty Officer Supervisors shall conduct periodic reviews to ensure that information is being entered correctly and consistently.
- (7) Self-Dispatch procedures
 - (a) The following types of calls shall continue to be performed over the radio:
 - 1. Any emergency situation or when the sworn member feels the radio is the most efficient means of communication.
 - 2. When a sworn member changes zones, he or she shall notify dispatch by radio.
 - 3. When a sworn member logs on duty for his or her assigned shift.
 - 4. When two or more sworn members are working together (10-12), they shall notify dispatch by radio at the beginning and end of their 10-12 times.
 - (b) When a member is working extra-duty employment at the beginning or end of his or her shift, he or she must log off-duty and back on duty between shifts. Self-dispatch may be used during extra-duty employment.
 - (c) The following commands are available for use with self-dispatch:
 - 1. Setting Unit Busy
 - 2. Setting Unit Available
 - 3. Setting Unit Enroute to an incident
 - 4. Setting Unit On-Scene at an incident
 - 5. Releasing Unit from an incident
 - 6. Creating a new incident
 - 7. Adding Notes/Persons/Vehicles/Vessels/Property to an incident
 - 8. Logging Off-Duty

9. Mode of Transportation

10. Secondary Activities

(8) Training

(a) Members designated as power users by the Fleet and Technical Services Section are available to conduct any training that is necessary.

G Procedures for Purchase and Use of Information Technology (IT) Equipment

- (1) In order to create and maintain efficiency and standardization, all computer hardware and software shall be approved by the Fleet and Technical Services Section in coordination with the Commission's Office of Information Technology (OIT) prior to purchase.
- (2) New and replacement computers for Division members shall be approved and purchased by the Fleet and Technical Services Section. Any IT equipment needs shall be communicated directly to the Fleet and Technical Services Section.
- (3) Each member shall have only one personal computer. Fleet and Technical Services Section approval is required prior to issuance of a second computer.
- (4) Cellular air card service shall be administered by the Fleet and Technical Services Section.
- (5) Internal cellular air cards are assigned to the computer and should not be removed except by trained staff. External cellular air cards or mifi devices are assigned to individual members. If a member with an external cellular air card or mifi device transfers to another position that requires the cellular air card, the member will keep the air card. If a member leaves the Division or transfers to a position that does not require the use of an air card, the supervisor shall send the device to Fleet and Technical Services to be disconnected.
- (6) If a member transfers within the same region or section, and the position the member is transferring to uses the same type of computer assigned as the one currently held by the member, the member's assigned laptop may transfer with the member. If the position the member transfers into has a different type of computer assigned to it, the member shall leave their assigned laptop. Computers assigned to a vacant position shall be returned to the Fleet and Technical Services Section for reassignment.
- (7) If a member transfers to a different region or section, and the position the member is transferring to uses the same type of computer assigned as the one currently held by the member, the member's assigned laptop may transfer with the member. If the region the member is transferring to does not have assigned computers, or has assigned computers of a different type, the member's assigned computer shall be returned to the Fleet and Technical Services Section for reassignment.
- (8) Computer vehicle mounts shall be approved and purchased by the Fleet and Technical Services Section. Computer vehicle mounts shall be removed from surplus vehicles, and refurbished and reinstalled into new vehicles whenever possible.
- (9) Mobile printers and other peripheral devices, including but not limited to cellular air card adapters, GPS antennae, and Driver License Scanners shall be supplied by the Region.

4 FORMS

FORM NUMBER	FORM TITLE
	Incident Summary Report
FWC/DLE-521	Division of Law Enforcement Memorandum