FORT MYERS POLICE DEPARTMENT
GENERAL ORDER 13.4

TITLE: Computer Usage & Records		
INDEXING: Computers Services, Computerized Records, Internet Usage, Intranet Usage, E-Mail Usage, Laptops (Laptops), Field Based Reporting		
ISSUED: 12/30/07	**REVISED:** 10/12/2023	**RESCINDS:** 06/02/2021
C.A.L.E.A. STANDARDS: 11, 41, 82	**C.F.A. STANDARDS:** 34	**PAGES:** 10

CONTENTS

This general order contains the following numbered sections:

PURPOSE

The purpose of this order is to establish guidelines for the access and usage of the Records Management System (RMS), the department's e-mail system, the Intranet, the Internet, D.A.V.I.D., E.L.V.I.S., L.C.S.O. Warrants page, NCIC/FCIC, the usage of the county's Universal Booking System, and any other technology resource designed for official City business.

SCOPE

These procedures shall apply to all Fort Myers Police Department personnel.

SECTION I: DEFINITIONS

A. CAD: The Fort Myers Police Department Computer-Aided Dispatch System.

B. D.A.V.I.D.: Drivers and Vehicle Information Database owned and operated by the Florida Department of Highway Safety and Motor Vehicles.

C. E.L.V.I.S.: Electronic License and Vehicle Information System

D. E-MAIL: A store and forward method of composing, sending, storing, and receiving messages over electronic communication systems.

E. HARDWARE: The physical components of a computer system including any peripheral equipment such as a printer, monitor, keyboard, and mouse.

F. INTERNET: The worldwide collection of electronic networks, online services, and various single-user computers by which users share information with other users through computer modems, cable lines, and telephone lines.

G. INTRANET: A private computer network that uses Internet protocols and network productivity to securely share part of an organization's information or operations with its employees.

H. L.C.S.O. Warrants Page: Lee County Sheriff's Office warrant/booking history access program.

I. MDT: Mobile Data Terminal or laptop

J. NCIC/FCIC: National Crime Information Center/Florida Crime Information Center

K. RMS: Records Management System

L. SOFTWARE: Computer programs containing instructions that tell the computer what operations to perform.

M. UBS: Universal Booking System application hosted by CJIS 20th Judicial Circuit for Lee County

N. VIRUS: A program that "infects" a computer. A virus can destroy or overwrite data, format or erase drives, or change a specific program.

SECTION II: ACCESS, RESTRICTIONS & PROHIBITIONS

A. User Access: (**C.A.L.E.A. 43.1.7a, 82.1.6) (CFA 34.12f,g)**

1. All requests for access to the department's computer system and/or any network server must go through the Support Services Division Lieutenant. **(C.A.L.E.A. 82.1.6c)**

2. When a new member requires access to the department's computer system and has been granted authority to the system by the Chief of Police or a member of the command staff, the member shall be added to the system with a user ID, password and correct authority level. **(C.A.L.E.A. 82.1.6c)**

3. User ID's and passwords may be changed at any time by the Computer Services Manager in response to a known or suspected security breach.

4. In order to maintain the integrity and security of records contained within the system, the department's Computer Services Manager will complete an annual password audit of the RMS. The Computer Services Manager will verify all passwords and access codes. **(C.A.L.E.A. 82.1.6d)**

5. An initial training session conducted by the Computer Services Manager or the Field Training Officer will be scheduled to instruct the member on how to login to the agency software and navigate through the appropriate menus and application options.

6. Members will be assigned a login and password to those programs in which they are authorized to access. **(C.A.L.E.A. 82.1.6c)**

7. Members will retain the confidentiality of their passwords to prevent unauthorized access. **(C.A.L.E.A. 82.1.6c)**

8. Passwords shall not be written down and stored in any un-secure location (Under keyboard or in an unlocked desk drawer). **(C.A.L.E.A. 82.1.6c)**

9. All members are allowed access to the Internet or Intranet through agency computers, once approved by the Computer Services Unit.

10. Members will not use the agency's computer system or any of its features to create, generate, perpetuate, comment on, or send any communication that is derogatory, demeaning, unprofessional, obscene, or harassing to any person or group.

11. All computer and Internet usage and usage of the department's e-mail system and other technology resources will also be in conformance with the City of Fort Myers Information Technology Services Technology Usage Procedure Manual.

B. Restrictions / Prohibitions: The following activities are, in general, prohibited or restricted with special permission required. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., a detective accessing a prohibited website for investigative purposes) Permission should be obtained in writing or by email prior to the prohibited access.

1. Under no circumstances is an employee of the Police Department authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the Police Departments technology resources.

2. Use of D.A.V.I.D., NCIC/FCIC, and E.L.V.I.S. will be according to the terms and conditions outlined in the user agreements and/or manual during application. **(CALEA 41.3.7b)**

3. All sworn personnel are permitted to use D.A.V.I.D./E.L.V.I.S. after proper application with D.H.S.M.V. and verification of employment by the "Agency Point of Contact". Civilian employees are permitted to use D.A.V.I.D./E.L.V.I.S. based upon their assigned position/duties in the agency. The Support Service Division Commander will grant and remove Civilian Employee access based on assignment. **(CALEA 43.1.7a)**

4. The use of the Records Management System (RMS), the department's e-mail system, the Intranet, the Internet, D.A.V.I.D., E.L.V.I.S., L.C.S.O. Warrants page, NCIC/FCIC, the usage of the county's Universal Booking System, and any other technology resource owned or operated by the city will be utilized for official City business only. (CFA 34.12 a,b)

5. Internet users are not permitted to engage in the following activities either during working or non-working hours, using City owned equipment or facilities:

   a. Access, retrieve, or print text and graphic information which exceed the bounds of generally accepted standards, good taste and ethics.

   b. Engage in activities which would in any way bring discredit to the Police Department.

   c. Engage in personal commercial activities on the Internet, including offering services or merchandise for sale.

   d. Engage in any activity which would compromise the security of any computer.

Employees shall have no expectation of privacy when using Department authorized or provided communications or computer systems.

Passwords assigned to or used by employees do not create an expectation of privacy for the employee but are used solely to prevent access by unauthorized persons.

The Department, with the assistance of ITS, will engage in the monitoring of electronic mail messages or other electronic files, documents, software, data, or electronic images created, downloaded, or accessed by employees, for valid purposes, including employee supervision. **(CALEA 41.3.7e)**

To ensure compliance with this policy, the Department reserves the right to inspect, monitor, remove, and read electronic messages, including computer files, caches, data, electronic mail, graphics, or digital photographs; to decipher encrypted files, text, and messages; and to remove or inspect software, especially software installed or altered without authorization.
(C.A.L.E.A. 11.4.4)

The Department is not obligated to obtain prior judicial approval before monitoring or accessing the communications systems described in this policy.

An employee's continued employment constitutes a waiver by the employee of any claims for infringement of privacy by the Department.

All Department computers, including all hardware, software, files, data, documents, caches, and electronic mail, are subject to random and unannounced inspections, at any time, by ITS or Police Department staff.

All employees have an obligation to report intentional or negligent violations of this directive by another employee to their supervisors.

Supervisors to whom violations of this directive are reported will take appropriate disciplinary action.

SECTION III: LAPTOPS/MDTs (C.A.L.E.A. 41.3.7) (CFA 34.12c)

A. Computer Services Manager’s Responsibilities:

1. The Computer Services Manager shall be responsible for the overall implementation, control, and maintenance of the laptop system.

B. Supervisor’s Responsibilities:

1. Assure their respective personnel are properly trained in the use of the laptop computer.

2. Assure the laptops are properly cared for, secured, and used in a fashion that is consistent with agency policy.

3. Conduct inspections of the laptops at least once a week to assure they are being properly maintained.

4. Those members that are assigned laptops, whether on a permanent or temporary basis, will be solely responsible for the care and safeguarding of the computer, the software therein and accessories.

5. Any damage to the laptops or problems with the programs should be reported immediately to the Computers Services Supervisor via the member’s chain of command.

6. Usage of department laptops shall be in conformance with the City of Fort Myers Information Technology Services Technology Usage Procedure Manual.

C. Usage Guidelines:

1. Global Positioning System (GPS): all sworn personnel and Community Service Aides are required to be signed into Mark43 First Responder Mode at all times while on duty. This applies to all personnel, when operating a department vehicle that is equipped with a laptop/MDT. This includes regular duty, overtime and off duty details. The only exception applies to members who are working in an administrative capacity (e.g., the Internal Affairs

Sergeant is not required to be signed in unless he/she is working in a patrol type function and/or working overtime or working an off-duty detail that could require responding to calls for service).

a. All personnel identified in section C.1. above, are required to verify their GPS is working properly by checking the location map regularly throughout their shift. Any discrepancies in location or outages will be immediately reported to their supervisor.

b. The vehicle number of the vehicle being utilized shall be entered into Mark43 First Responder Mode. If the vehicle does not have an MDT, personnel must provide their vehicle number to the Communications Division when beginning their tour of duty, overtime or off duty detail.

c. Disabling or attempting to disable GPS is not permitted. Personnel not following this procedure will be subject to disciplinary action up to and including termination.

2. Primary use of the laptops is intended for the writing and transmission of reports.

3. Laptops are to be used for official City business only.

4. For the safety of the user and citizens nearby, laptops SHALL NOT be used, read, or typed on while the patrol vehicle is in motion**.**

a. The patrol vehicle must be at a complete stop or legally parked for the user to view or access information on the laptop.

5. To minimize undue wear and tear on the laptops, members will do the following:

a. Use only authorized accessories and/or components (Adapters, batteries, fuses, etc.) that have been issued by the department.

1. Failure to do so will result in the member being responsible for damages caused to the notebook by un-authorized accessories.

6. Members going off-duty should log off the system completely and turn off the laptop.

7. The member shall not, under any circumstances, leave laptops in the vehicle’s trunk.

8. The laptop shall be maintained by the assigned member, as outlined in this general order.

a. Failure to maintain the battery properly will affect the performance of the notebook computer.

9. Certain needs of the department dictate assignment of laptops to specific personnel.

10. The Computer Services Manager, or designee, shall assign laptops and provide the description, serial number, and property number of the unit assigned for fixed asset control purposes.

11. Members will return their laptop and all accessories to the Computer Services Manager leaving the employment of the Fort Myers Police Department or if they are called to military active duty resulting in an absence longer than (14) days.

12. Violations of any aspect of this order shall result in disciplinary action.

a. Disciplinary action may include but is not limited to progressive discipline and/or the loss of the permanent assignment of a laptop.

13. Spare Laptops: The police department does not have any spare laptops for temporary assignment to members. All laptops are issued directly to personnel and/or assigned to department vehicles. Future budgets may allow the agency to maintain a pool of spare laptops.

SECTION IV: RECORDS MANAGEMENT SYSTEM (RMS)

A. Computerized Records Management System (RMS):

1. The Automated Records Management System of the Fort Myers Police Department consists of an officer-based incident report methodology.

a. This system contains the agency's historical and current information database in perpetuity.

b. Information from preliminary Offense Incident Reports, Traffic Crash Reports, Follow-up Reports (Supplementary), and Arrest Affidavit Reports is entered by the officer and sent to a supervisor. Once a supervisor reviews and approves the report, it is then sent to the Records Section.

B. All initial and supplemental reports will be completed on the computers as opposed to handwritten, unless circumstances preclude, and then only when authorized by a supervisor.

C. RMS: All Incident, Narrative, Persons, Property, Vehicle, and Supplemental Reports will be completed in RMS. This includes all supplemental reports that may be completed after the initial report is submitted. All personnel responsible for completing these documents can utilize either a laptop or desktop computer to complete the reports. When the computer systems/RMS is down or malfunctioning, hard copies will be completed and turned into the Records Section. **(C.A.L.E.A. 82.2.1a,b,d)**

D. UCR/Part One Crimes: Officers responding to a report of a part one crime shall investigate and file a report. The following are part one crimes, which must be reported to ***NIBRS/FIBRS*** for Uniform Crime Reports (UCR). **(C.A.L.E.A. 82.2.1a,b,d)**

1. Murder
2. Sex Offenses
3. Robbery
4. Aggravated Assault / Battery and Stalking
5. Burglar
6. Thefts / Larceny
7. Auto Thefts

E. In addition to the above offenses, the following shall be reported using the offense report. If the reporting officer has questions whether an offense report should be generated, they shall contact their immediate supervisor. **(C.A.L.E.A. 82.2.1a,d)**

1. Arson
2. Domestic Violence

3. All felony crimes that do not have arrests

4. Missing Children and Endangered Adults
5. Criminal Mischief
6. Other miscellaneous calls for service (Death Investigations, etc.)

F. Information Required: (**C.A.L.E.A. 82.2.1c, d)**

1. Completion of Reports and Follow-up Reports:

a. Reports and Follow-up reports are used to document certain incidents (listed above), or to report any additional information pertinent to an original report utilizing the original report number.

b. Officers will complete Reports and Follow-up reports to properly document incidents. Such reports will contain all of the necessary details of offenses or incidents.

c. Reports will be completed and submitted to an immediate supervisor prior to going off-duty, unless specifically excused by the supervisor. This is required for both computer-generated reports and handwritten reports. **(C.A.L.E.A. 82.2.1a)**

G. Telephone Reporting: The Department will provide assistance to the public by handling calls for service via the telephone for incidents or situations that do not require the physical presence of a police officer, thus making police officers available for higher priority calls. Officers and Community Service Aides may take a complaint by telephone if all of the following criteria are met: (**C.A.L.E.A. 82.2.5)**

1. Suspects have left the scene and their whereabouts are unknown.
2. There is no need for an Officer or CSA to be present at the scene.
3. The caller is receptive to giving the report over the telephone.

The following types of calls, with supervisory discretion, may be considered for reporting by telephone:

1. Grand Theft Auto
2. Internet Fraud
3. Burglary Auto
4. Credit Card Theft
5. Theft:

a. From Auto
b. Auto Parts
c. From Boat
d. Of Bicycle
e. Pick Pocket
f. From Vending Machine
g. Petit Theft

6. Grand Theft, usually $1,000 or less; if there is no crime scene or suspects
7. Gas drive off – report taken over the telephone and BOLO issued on the vehicle.
8. Missing Person: Adult, unless endangered
9. Telephone Calls:

a. Obscene/Harassing

b. Threatening – unless: There is an indication that the perpetrator is enroute to harm the complainant or Complaint is domestic related.

10. Lost Property
11. Vandalism
12. Fraudulent Use of Credit Cards
13. Theft from Building

H. While conducting an investigation of a Part One Crime, the investigating officer determines that the victim is intoxicated or under the influence of narcotics to the extent that the investigating officer feels the victim is incapable of assisting with the investigation, the officer shall advise the victim to contact the police department when they are no longer intoxicated. This applies only when there are no witnesses to the offense who can corroborate the victim's story.

I. RMS Procedures: (**C.A.L.E.A. 82.2.1d,e)**

1. When reports are completed in the RMS System, Officers and Community Service Aides will forward the report electronically to their supervisor, or another on-duty supervisor for review and approval.

2. If no corrections are needed, the reviewing supervisor will then approve the report and it will be forwarded to the Records Section. If corrections are needed, the reviewing supervisor will reject the report so that the employee can make the appropriate correction. Once corrections are made, the employee will forward the report back to the supervisor.

3. NCIC/FCIC Entry – If a report contains information to be entered into NCIC/FCIC, personnel completing the report, will use the Labels "Action Required" FCIC/NCIC entry. This is accomplished by adding the Label "Action Required: FCIC/NCIS Entry" located in the upper right-hand corner of the Offense Report in Mark 43. This will alert the Communications Section that an entry is required. Communications personnel will remove this label after entry and replace it with "Completed: FCIC/NCIC Entry".

J. Mark43 RMS & Universal Booking System (UBS): All arrest reports for arrestees will be completed electronically within the Mark43 RMS and will be transmitted via an interface to the Lee County Universal Booking System (UBS). Officers can utilize either the desktop computers in the station, or the desktop computers at the Lee County Jail.

1. The Notary Section in UBS shall be completed to including the date, notary officer's name, and ID number. Handwritten dates or names cannot be used.

SECTION V: COMPUTER MAINTENANCE, BACKUP & SECURITY

A. Computer File Maintenance, Backup, and Retention:

1. Security for Networking Components and Computer System:

a. The Computer Services Manager is responsible for security and service of the electronic data processing system. **(C.A.L.E.A. 82.1.6c)**

b. The security safeguards control what personnel can use the devices, data, and programs. It also prevents accidental or intentional destruction of the system resources **(C.A.L.E.A. 82.1.6c).** All software shared via any network server is to be protected by anti-virus software and regular data backups. **(CFA 34.12e)**

c. Browser based software is to be installed / updated with the latest versions of secured, encrypted software and service packs available.

B. Protection of Network / System Data: (**C.A.L.E.A. 82.1.6a,b)**

1. The Computer Services Manager is required to protect agency electronic data processing information by performing a daily "backup" or "save" procedure.

2. This "save" procedure copies the organization's data to digital media.

3. Server resources are backed up daily onto digital media which is hard drive based.

4. Fiber optic communications is used to back up the data to an offsite server location in a building rated at wind resistance of greater than 130 miles per hour. Only Police Department and City of Fort Myers ITS personnel have access to this server room.

5. A set of system backup media is kept in the Computer Services Office.

6. All data, which resides on the agency's network servers as "shared folders" will be backed up on a daily basis.

7. The backup processes are scheduled and maintained by the Computer Services Manager.

C. Retention and Archiving of Electronic Data: (**C.A.L.E.A. 82.1.6a)**

1. The Computer Services Manager will ensure that retention, archiving, and purging of electronic data is accomplished in accordance with agency policy and procedures. The following standards will increase the performance, efficiency, and useful life of the agency's current series system, as well as all network servers.

2. The Records Section shall ensure:

a. Retention of historical and current data is held in perpetuity.

b. Electronic records data is not purged.

3. Command Staff & Revoking Access: **(C.A.L.E.A. 82.1.6c)**

a. Whenever a member's access to the agency's computer system must be revoked, or the member's access level modified, all instructions shall come from the Computer Services Manager or designee.

b. Additionally, a member's access shall be immediately revoked when he / she leaves the agency's employment.

c. The Chief of Police, the command staff, and other authorized individuals also have the ability to retrieve general or specific information from one or all field reports to generate monthly reports, conduct manpower studies, and to complete other reports.

SECTION VI: HARDWARE & SOFTWARE

A. Members will not make any additions, changes, or deletions to ANY department computer's hardware, software, or peripheral systems. All such changes are the responsibility of Computer Services. **(C.A.L.E.A. 11.4.4) (C.A.L.E.A. 41.3.7c,d) (CFA 34.12d)**

B. Computers and related equipment will be repaired and configured by Computer Services personnel only.

C. Members will not move desktop computers or computer related equipment. Relocations are the responsibility of Computer Services personnel.

D. Members should use extreme caution when eating or drinking at a computer workstation. If any liquid is spilled on the computer system, the user should logout immediately, turn off all power, wipe up the spill quickly, and advise Computer Services.

E. All computer related requests will be submitted through the Computer Services "Help Desk" located on the Departments intranet page.

REFERENCES:

City of Fort Myers Information Technology Services Technology Usage Procedure Manual RMS Manual.

APPROVED:

[DIGITAL SIGNATURE ON FILE]	**10/12/2023**
Jason Fields, Chief of Police **Fort Myers Police Department**	**Date**