


# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

	<b>TITLE</b> Access and Use of City Computer Systems	<b>ACCREDITATION</b> CALEA Chapter 11.4.4, 41.3.7, 82.1.6	
	<b>PROponent UNIT</b> Information Technology (IT) Division	<b>PRIOR REVISIONS</b> 10/01/01, 6/24/02, 7/17/08 <b>ATTACHMENT: 0</b>	
<b>NUMBER</b> 40.29	<b>ISSUE DATE</b> 12/21/98	<b>REVISION DATE</b> 05/04/2020	<b>TOTAL PAGES</b> 16

**I. PURPOSE:** The purpose of this order is to set general guidelines for access and use of the City's computer network including Internet access, procedural guidelines for the use and protection of the Gainesville Police Department's computer and laptop systems, including both software and hardware components and the use and regulation of files, related applications and all identified restrictions of use.

**II. POLICY:** Department personnel shall refer and adhere to the City of Gainesville Use of Information Technology Systems and Resources (H.R. police G-7) and this General Order, regarding City computer, Internet and e-mail usage. No member of this Department should attempt to use a computer or software applications without proper training. Improper use could result in a serious compromise of the system and software and/or disciplinary action.

All software, operating systems, files and related applications are licensed to and are considered to be under the control of the City of Gainesville and the Gainesville Police Department. Additionally, all hardware on which the above mentioned is installed or operated from is under the control and ownership of the City of Gainesville and the Gainesville Police Department.

In order to ensure the integrity of the Criminal Justice Information System (CJIS) network, as well as the computer and laptop systems, no one is permitted to load/install or review any computer application software – regardless of whether or not the software is on a factory disk-without first obtaining approval from the Information Technology Department (I.T.). This is to help prevent any software conflicts, as well as act as a preventive measure against computer viruses. Each member of this Department will be held accountable for the proper use of the system. Members will be held liable for the misuse of any police related information. Each member has a moral and legal obligation to manage information with great care.

Messages that are created or received in the transaction of official business and retained as evidence of official policies, actions, decisions or transactions are Public Record. Employees shall have no expectation of privacy when using Department issued computer systems.

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

### **III. DEFINITIONS:**

**CAD**: The Gainesville Police Department Computer-Aided Dispatch System.

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

**LPR**: License Plate Recognition System.

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

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

**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.

**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.

**MDT**: Mobile Data Terminal or Laptop.

**Public Records**: Messages that are created or received in the transaction of official business and retained as evidence of official policies, actions, decisions or transactions.

**RMS**: records management system

### **IV. PROCEDURE:**

**A. Access, Restrictions and Prohibitions (Establishing and Terminating Employee Computer / E-Mail Accounts)**: I.T. is responsible for ensuring Domain and email account activations/ deactivations for new hires and terminating employees.

**1. User Access**: [CALEA 41.3.7.a & 82.1.6]. All requests for access to the department's computer application and/or any network server must go through the I.T. [CALEA 82.1.6.c]

i. 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. [CALEA 82.1.6.c]

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

- ii. The Personnel Services Division will notify the IT Dept. when the necessary accounts need to be established.
- iii. The City of Gainesville's I.T. personnel will advise GPD Personnel that the accounts have been created.
- iv. User ID's and passwords may be changed at any time by the I.T. Dept. in response to a known or suspected security breach.
- v. I.T. will create any departmental system accounts or permissions, and advise the employee of the account name and initial temporary password.
- vi. The way the account and permissions are established, is normally related to the member's duties and responsibilities, and will indicate the relevant access the member has, to programs on the system.
- vii. Expanded or additional access to programs, will depend on the member's assignment and/or change in assignment. Approval from his/her commander may be required.
- viii. The designated member of the Personnel Services Division will ensure that I.T. Dept. receives timely notification when a Department member is terminated or when other action occurs that would cause a person's computer access to become invalid.
- ix. An initial training session conducted by I.T. or designee will be scheduled, to instruct the member on how to login to the agency software and navigate through the appropriate menus and application options.
- x. Members will be assigned a login and password to those programs in which they are authorized to access. [CALEA 82.1.6.c] Members will retain the confidentiality of their passwords to prevent unauthorized access. [CALEA 82.1.6.c]
- xi. Passwords shall not be written down and stored in any un-secure location (Under keyboard or in an unlocked desk drawer). [CALEA 82.1.6.c]

**B. Authorized Use:** In compliance with the City's Automation Standards, City computers and computer systems are to be used for work-related purposes. [CALEA 41.3.7.b]

- 1. Members may use their department computer for personal use limited to 15 minutes per week. All computer and Internet usage and usage of the

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

department's e-mail system and other technology resources, will be in conformance with the City of Gainesville Information Technology Services Usage Procedure Manual.

2. Legitimate job responsibilities (e.g., a detective accessing a prohibited website for investigative purposes) Permission should be obtained in writing or by email from appropriate chain of command prior to the prohibited access.

### **C. Internet Use and Requests for Internet Access:**

1. For individuals who do not have, but who need internet access: The supervising division / bureau commander shall inform I.T. of each individual under their command for whom access is desired. I.T. will activate any accounts requested by the division / bureau commander.
2. Internet E-mail: The approved electronic mail software program is Microsoft Outlook.

### **D. Restrictions / Prohibitions: Permission should be obtained in writing or email prior to prohibited access being undertaken.** The following activities are, in general, prohibited or restricted with special permission required.

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. Except for a bona fide, approved law enforcement purpose, members shall not use City computers to visit sites on the Internet that are inappropriate in the workplace

Examples include (but are not limited to) sites with games, pornography, gambling, etc. 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).

3. Internet users are not permitted to engage in the following activities either during working or non-working hours, using City owned equipment or facilities:
  - i. Access, retrieve, or print text and graphic information which exceed the bounds of generally accepted standards, good taste and ethics.
  - ii. Engage in activities which would in any way bring discredit to the Police Department.

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

- iii. Engage in personal commercial activities on the Internet, including offering services or merchandise for sale.
- iv. 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.
- v. Use of department issued laptops outside of normal working hours needs to be approved by the relevant chain of command.
- vi. Department members will not add, remove, update or alter any programs on the Department issues laptop or computer.

### **4. Exceptions:**

- i. Members who are assigned a laptop may use their assigned GPD laptop or agency computer for their personal educational endeavors under the following guidelines:
  - ii. Laptops or agency computers will not be directly connected (wired or wirelessly) to any network other than the city network. Member may connect to other networks (wired or wirelessly) but first must ensure the information is encrypted through the department Virtual Private Network (VPN). Bypassing the VPN will only be completed with prior approval from the I.T. Supervisor.
5. Members shall not use the City 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 [See GOs 22.8, 26.1, 26.3]
6. Use of D.A.V.I.D., NCIC/FCIC, LInX, Finder, and LPR will be according to the terms and conditions outlined in the user agreements and/or manual during application. [CALEA 41.3.7.b]
- i. All sworn personnel are permitted to use D.A.V.I.D./LPR after proper application with D.H.S.M.V. and verification of employment by the "Agency Point of Contact".
  - ii. Civilian employees are not permitted to use D.A.V.I.D./LPR. Without prior written permission from their Bureau Commander. Written permission can be in the form of an email or memorandum. The "Agency Point of Contact" will retain all approved civilian requests for access and ensure compliance with this policy before allowing access. [CALEA 41.3.7.a]

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

- iii. The use of the Records Management System (RMS), the department's e-mail system, the Intranet, the Internet, D.A.V.I.D., LPR, LInX, P2P, Finder, NCIC/FCIC, and any other technology resource owned or operated by the City will be utilized for official City business only.

**E. Authorized Internet Use:** The Gainesville Police Department I.T. Department provides Internet access to the Gainesville Police Department. No other Internet services are authorized for loading or use on City computers.

**1. Internet System Monitoring:** Is done on an as needed basis, depending on known risks or at the request of a supervisor.

**2. Commanders' Responsibilities:** The commander will review the information, determine whether the site visit(s) were appropriate, and, within 3 weeks, report his/her findings and/or actions taken to I.T. via an IOC or e-mail.

If the supervising commander believes misconduct has occurred, he/she is responsible for coordinating with Internal Affairs regarding appropriate action.

**3. Prior Notice to Division Commander:** Members who have a legitimate need to visit a site that may be considered inappropriate shall notify their Division Commander in writing (IOC, e-mail) within four hours of accessing the site, to avoid triggering the command review process. Members should inform their supervising commander prior to visiting the site. Members will be held accountable if access is later determined not to have been for a legitimate need.

**Exception:** I.T. Supervisor may approve exception(s) at remote sites where City network access is not available, or when necessary for investigative purposes.

**F. Electronic mail monitoring:** The City/GRU Information Technology group will engage in the monitoring of electronic mail messages and Gainesville Police Department I.T. will monitor electronic files, documents, software, data, or electronic images created, downloaded, or accessed by employees, for valid purposes, including employee supervision. [CALEA 41.3.7.e].

**1.** Correspondence that is created or received by members of the Department in connection with official business, including mobile data computer instant messages, is subject to records access and management laws and regulations as outlined in Chapter 119 of the Florida State Statutes.

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

2. 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. [CALEA 11.4.4]
3. 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.
4. 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.

### **G. Employee Required Tasks/Duties:**

1. **Passwords:** Individuals select their own passwords for access to the various computer systems.
2. Members must change the temporary password initially issued to them by I.T. to one of their own choosing.
3. Members shall retain the confidentiality of their passwords to prevent unauthorized access.
4. Members are specifically prohibited from prominently displaying any computer system passwords on or about their computer or office workstations.

**H. Annual Audit:** At least once each year, I.T. personnel shall audit the Department's computer system, including passwords, to ensure that only current employees and other authorized persons have appropriate computer access. IT will verify all passwords and access codes [CALEA 82.1.6.d]

**I. System File Backup & Security:** The following procedures and guidelines shall be in place for Department computer system files, back-up and storage. 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 IT or other Police Department staff. [CALEA 82.1.6.a & 82.1.6.b]

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

- 1. Computer Aided Dispatch (CAD):** The Alachua County Sheriff's Office is responsible for data files, back-up and storage in the Records and Communications CAD computer systems that record relevant GPD data.
- 2. GPD Servers and Computer Resources Managers:** I.T. personnel and City Computer Services personnel are responsible for ensuring and/or coordinating the maintenance, back-up and storage of data on the City and Department servers.
- 3.** Related procedures can be found with the Sheriff's Office Information Technology personnel.

### **J. Computer File Maintenance, Backup & Security.**

#### **1. Security for Networking Components and Computer System:**

- i. The I.T. Manager is responsible for protection, security, retention, maintenance and service of the network and electronic data processing system. [CALEA 82.1.6.c]
- ii. The security safeguards control what personnel can use the devices, data, and programs. It also prevents accidental or intentional destruction of the system resources [CALEA 82.1.6.c]. All software shared via any network server is to be protected by anti-virus software and regular data backups.
- iii. Browser based software is to be installed / updated with the latest versions of secured, encrypted software and service packs available.

#### **2. Protection of Network / System Data:** The I.T. Manager is required to protect agency electronic data processing information by performing a daily "backup" or "save" procedure: [CALEA 82.1.6.a & 82.1.6.b]

- i. This "save" procedure copies the organization's data to digital media.
- ii. Server resources are backed up daily onto digital media which is hard drive based.
- iii. 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.
- iv. Only Police Department and City personnel that have been cleared by Gainesville Police Department have access to this server room.



# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

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

3. The I.T. 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.[CALEA 82.1.6.a]

i. The Records Section shall ensure:

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

b. Electronic records data is not purged.

ii. Command Staff & Revoking Access: [CALEA 82.1.6.c]

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 I.T. 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.

iii. Virus Detection Software: The Department has an anti-virus server that rolls out virus detection updates automatically to each PC (personal computer) for protection against viral infections.

iv. System Back-Ups: Nightly back-ups of all data on City and Department servers shall be performed.

v. Storage: All backup media is off site at a secure location.

vi. Media Disposal: Discarded media, including back-up media (tapes) shall be rendered unusable / unreadable prior to disposal.

### **K. Electronic Mail System (E-mail), Software, and Internet Usage.**

1. Authorized uses of email in the workplace:

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

- i. Facilitate performance of job functions.
- ii. Facilitate the communication of job related information in a timely manner.
- iii. Coordinate resources, locations, and individuals for agency meetings.
- iv. Communicate with departments throughout the City regarding job related matters.
- v. Communicate with outside organizations as required to perform job functions

**2. Unauthorized uses of e-mail and internet:** These include, but are not limited to, the following:

- i. Personal usage.
- ii. Transmission of confidential information.
- iii. Use in violation of any federal, state, or local law.
- iv. Communications containing threats, or harassing, or intimidating statements.
- v. Communications containing defaming, slanderous, or libelous statements.
- vi. Obscene, offensive, or suggestive messages or graphical images.
- vii. Racial, religious, ethnic, or sexual slurs.
- viii. Possession, storage, or transmission of messages containing nudity, pornography, child pornography, or other images, words, or language that are sexually explicit, or of a prurient or sexually suggestive nature; unless necessary as part of a criminal investigation approved by the Chief of Police or his designee.
- ix. Political endorsements.
- x. Commercial activities or solicitations.
- xi. Chain letters.
- xii. Misrepresenting one's identity while using e-mail.

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

- xiii.** Intercepting, disrupting, or altering electronic communications.
  - xiv.** Criticizing Department management and/or policy decisions; or disseminating opinions and/or promoting philosophies contrary to management policies.
  - xv.** Sending copies of documents in violation of copyright laws.
  - xvi.** Compromising the integrity of the Department and its business in any manner.
  - xvii.** Using the electronic mail system for overtime jobs, job searches, or the advertisement of personal business.
- 3. Email Signature:** City of Gainesville email addresses signature lines shall not have any additional information beyond contact information and public records disclosure. Quotes, phrases, memes, references, photographs or other information not related to contact information or the public records notice are not permitted.

### **L. MDT (Laptop):** [CALEA 41.3.7]

- 1. System Design:** The MDT system is a computer-based system that uses a laptop computer which can be mounted in a patrol car. Cellular communications and modems connect the users to the system.
- i.** The MDT system allows the user to send and receive voiceless messages to and from other users. Users include other Gainesville Police Department mobile users, the Communications Center, and other authorized law enforcement users.
  - ii.** The MDT system is designed to access the Criminal Justice Information System, Florida Crime Information Computer (FCIC), National Crime Information Center (NCIC), National Law Enforcement Telecommunications System (NLETS), and the Florida Division of Motor Vehicle (DMV). A computer interface will allow mobile users to receive dispatches through our Computer Aided Dispatch (CAD) system and to access our Records Management System (RMS), Field Reporting, Accident and Investigations.
- 2. System Administration:** I.T. Department is responsible for the administration of the MDT system and shall coordinate all activity involving

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

the MDT and ensure all records associated with the system are maintained.

### **3. System Security:**

- i. All information received through the CJIS system (FCIC, NCIC, NLETS and DMV) is confidential. Only authorized criminal justice agencies may request and receive this information.
- ii. Every transaction that goes through the computer system (computer and laptop) is recorded and is subject to discovery for court purposes and is governed by Public Records. Department members shall follow proper protocol when using the system.
- iii. The laptop computer may be used to access information regulated by state and federal law from the Florida Crime Information Center and the National Crime Information Center (FCIC/NCIC) under the following conditions:
  - iv. Use of information is solely limited to law enforcement purposes, since the dissemination of information to non-law enforcement is unauthorized and unlawful.
  - v. Access is limited to Department members who have completed authorized training and are certified as established by the Florida Department of Law Enforcement (FDLE).
  - vi. Laptops may be used for vehicle-to-vehicle or vehicle to station communication.
  - vii. The Federal Communications Commission (FCC) regulates all wireless transmissions.
  - viii. Members are prohibited from transmitting messages that are not official law enforcement business (contain inappropriate language, are harassing or discriminatory, or otherwise considered unprofessional).
  - ix. The Department will allow the member to use his/her assigned laptop while he/she is off-duty under the following conditions for all circumstances:
    - a. Additional software programs will not be loaded unless authorized by I.T. Department [CALEA 41.3.7.c]
    - b. Games may not be loaded or used.

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

- c. Only I.T. personnel or designee will install any approved software.
- d. Hardware items are not to be removed or added to the laptop unless authorized by I.T.
- e. Only I.T. personnel may alter, modify, or delete existing configurations, files, systems, and like contents on the member's laptop computer. [CALEA 41.3.7.d]
- f. Department files and programs take precedence over a member's personal files and programs.
- g. Personal files and programs may have to be deleted to make room for Department files and programs.
- h. Members are prohibited from hiding or password protecting files.
- i. No member shall connect to the Internet except through the Gainesville Police Department connection unless authorized by I.T. Division
- j. Each Department Member will have his or her own password to logon to the system. When the police car is secured at the end of the department member's tour of duty, the user will log off the system.

#### **4. Laptop (MDT) Inquiries:**

- i. Department members shall use the laptop (MDT) system in the following manner:
  - a. To obtain information for an investigation or other police purpose.
  - b. To obtain information concerning a suspicious person, vehicle, or article.
- ii. Department members shall not use the laptop (MDT) system to obtain information for unauthorized persons and/or for non-law enforcement purposes.

#### **5. System Operation:** Department members shall not operate the laptop (MDT) while the police car is in motion.

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

**6.** To prevent unauthorized viewing of sensitive, police related information on the laptop (MDT), members shall take the following precautions when leaving the patrol car and laptop (MDT) unattended:

- i. The member shall not leave the laptop in FCIC, NLETS mode.
- ii. The member shall lock and secure the police vehicle.
- iii. At the end of shift the member shall secure their laptop in the trunk of their vehicle or inside their place of residence.

### **7. Care and Maintenance of the Laptop Computer:**

- i. The laptop (MDT) is a sensitive piece of electronic equipment. Fluids, dirt, and other foreign material will affect the ability of the unit to function properly.
- ii. The laptop (MDT) has a liquid crystal display (LCD) screen. The LCD screen can be punctured easily. If the screen is damaged, the unit will have to be taken out of service. Members should be careful not to close the laptop with items on the keyboard.
  - a. Members are responsible for the care and maintenance of their assigned laptop (MDT).
  - b. Damage to the laptop of any kind requires members to immediately forward a detailed memorandum to I.T Department through their immediate supervisor and chain of command.
  - c. If the laptop (MDT) does not operate, the member will turn it over to I.T. Department with a copy of the memorandum forwarded to their supervisor.
  - d. When the laptop (MDT) is not damaged, but is malfunctioning, the member's immediate supervisor shall be made aware of the situation and the equipment shall then be forwarded to I.T Department. If available, a spare laptop (MDT) may be temporarily issued.
  - e. If the malfunction occurs after regular business hours or on weekends, members may check out a loaner laptop (MDT) via an Operations shift supervisor or Shift Commander. This shall be returned by the member at the end of their shift.
  - f. The member shall clean the laptop screen only as follows:

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

1). Turn the laptop (MDT) OFF.

2). Use a lint-free cloth to gently wipe the screen.

3). Follow the laptop manufacturer's directions, which are included with the laptop. Do not use water, soap, Windex, etc.

g. The member shall clean the laptop keyboard and case as follows:

1). Turn the laptop (MDT) OFF.

2). Spray commercial computer keyboard cleaner onto a lint-free cloth and wipe the keyboard.

3). Do not spray the cleaner directly onto the keyboard.

4). Do not use the spray on the screen.

iii. **Automatic Vehicle Locator (AVL)**: Each mobile data computer (MDC) is equipped with global positioning system (GPS) software, known as AVL. In conjunction with a GPS receiver/antennae, AVL records and tracks location information. AVL serves to locate members who may be in need of assistance and to improve response-times by the efficient deployment of resources.

a. Members shall not deliberately tamper with the AVL system or attempt to hinder the system's designated performance.

b. Members shall not deliberately disconnect the GPS receiver/antennae from the MDC unless it is for the purposes of removing the MDC from the vehicle.

**Exception:** FTOs are not required to have their assigned MDC connected to the GPS receiver/antennae if theirs is the secondary MDC in the vehicle and the trainee's MDC is configured to function as the primary responding unit and is connected to the GPS receiver/antennae.

c. Members shall immediately report problems with the AVL to their supervisor and to the Information Technology Section.

d. Violations of this order shall be considered a Major Offense and will subject members to disciplinary action (see G.O. 26.1 and G.O. 26.5).

# **GAINESVILLE POLICE DEPARTMENT**

## **GENERAL ORDER**

### **8. Inspections:**

- i. Department supervisors shall inspect laptop (MDT) during periodic and scheduled equipment inspections and document any damage that is observed. Additionally, inspections of hardware and software by supervisors may be conducted any time a supervisor deems necessary. [CALEA 41.3.7.e]
- ii. The I.T. Supervisor shall have the functional authority to inspect any member's laptop (MDT), software and computer files at any time.

### **9. MDT System shutdown procedure:**

- i. The Department member will exit all CAD and mobile field reporting operations.
- ii. Upon logging off the CAD/MFR operations, the department member will exit the MS WINDOWS operating system and properly shut down the laptop.

### **10. Supervisor's Responsibilities:**

- i. Ensure their respective personnel are properly trained in the use of the laptop (MDT)
- ii. Ensure the laptops are properly cared for, secured, and used in a fashion that is consistent.

**M. Usage Guidelines:** Members will return their laptop (MDT) and all accessories to I.T. when leaving the employment of the Gainesville Police Department or if they are called to military active duty resulting in an absence longer than (14) days (G.O. 40.29 Computer Usage & Records). Violations of any aspect of this order shall result in disciplinary action. Disciplinary action may include, but is not limited to progressive discipline and/or the loss of the permanent assignment of a laptop.

---

**By Order of**

*Signed Original on File in the  
Accreditation Unit*

---

**Tony R. Jones  
Chief of Police**