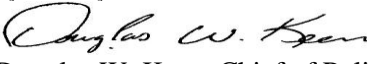




City of Manassas Police Department

General Duty Manual



Effective Date: 07-21-2014	GENERAL ORDER	Number: 04-03
Subject: Computer Systems		
<input type="checkbox"/> New <input checked="" type="checkbox"/> Amends <input type="checkbox"/> Rescinds <input checked="" type="checkbox"/> Reviewed: 02/01/2025		Reevaluation: <input type="checkbox"/> 1 yr. <input type="checkbox"/> 18 months <input checked="" type="checkbox"/> 24 Months
Accreditation Standards: 11.4.4/ 41.3.7/ 81.2.8/ 82.1.1/ 82.1.2/ 82.1.6	By Authority Of:  Douglas W. Keen, Chief of Police	Total Pages: 5

PURPOSE:

To provide guidelines for access to and use of Department computer systems.

POLICY:

All sworn members and selected non-sworn members are granted access to the various City and Department computer systems for enhanced communication and data processing, and to provide members with access to the Department, City and State databases. All sworn members of the rank of Sergeant and above, and other selected sworn and non-sworn members are issued personal computers or laptop computers, for enhanced communication and data processing, and to provide members with access to the Department, City and State databases.

The Department installs mobile computers in most emergency vehicles as practicable, and selected other fleet vehicles, and connects mobile computers to the Department Computer-Aided Dispatch (CAD) System, in order to facilitate efficient law enforcement response to incidents and provide members with access to the Department, City and State databases.

DISCUSSION:

N/A

PROCEDURE:

I. Systems Management

- A. The City's Information Technology Division (hereafter referred to as City IT) has the primary responsibility for installation, maintenance and repair of the Department's computer systems. The Technical Services Sergeant is the Department's Systems Manager and is responsible for working with current or potential users of the Department's computers to assist them in understanding particular application requirements or information needs.
- B. The Records Manager is the backup Systems Manager.
- C. Members needing assistance with the Department's AS/400 System applications meet with the Technical Services Sergeant, or the Records Manager, and discuss the request and service needed. Examples of the types of assistance and services that can be requested are:
 1. New systems.
 2. System redesign / modification for "CRIMES" software is provided by the Records Manager.
 3. Hardware services.
 4. The Records Manager provides in-house training for "CRIMES" and CAD Software (for non-PSCC members).
- D. The Technical Services Sergeant or the Records Manager assigns members their user name designation and specific instructions on creating passwords for entry into the Department's AS/400 System.
- E. Relevant computer specialty manuals are periodically prepared and issued to members by the Technical Services Sergeant, the Records Manager or other authority. Other in-house training is provided by the Records Manager.

Effective Date: 07-21-2014	GENERAL ORDER	Number: 04-03
Subject: Computer Systems		Page: 2 of 5

- F. System problems and critical system failures are reported to the Technical Services Sergeant, who schedules or affects the appropriate repairs. In the event of critical system failures after hours, City IT should be contacted directly

II. Computer Systems, Generally

- A. The Department's IBM Mid-Range Computer (AS/400) is linked to the City's Local Area Network system for most computer applications, and is hereafter known collectively as "the System."
- B. Configuration of the System. The System is comprised of various subsystems for Department use, including:
 - 1. The City Local Area Network (including the City Local Area Network Mail Server).
 - 2. The Department IBM Mid-Range Computer.
 - 3. The Computer-Aided Dispatch (CAD) system.
 - 4. The Mobile Data Terminal system.
 - 5. Personal Computers.
- C. Records Management, generally.
 - 1. Records management system, containing:
 - a. CAD (Computer Aided Dispatching).
 - b. "CRIMES" Software.
- D. NCIC / VCIN
 - 1. The Department is linked to NCIC and VCIN through terminals located in the Public Safety Communications Center (PSCC), accessed by "GLINK" Software, and routed to Mobile Data Terminal (MDT) System computers mounted in the Department's fleet vehicles and on selected desk top computers.
 - a. NCIC/VCIN also interfaces with the MDT System by linking to the AS/400.
 - 2. Use of these terminals must be in accordance with all applicable manuals and directives provided by the FBI and the Virginia State Police.
 - 3. In the event that a system failure occurs, on-duty PSCC members contact VCIN Control in Richmond by telephone. VCIN Control can advise if the failure is system-wide or a local problem.
 - a. In the event that the failure is a local problem, PSCC members contact the Technical Services Sergeant to coordinate the system being brought back on line.
 - b. The City Information Technology Division is contacted for "GLINK" PC failures.
 - c. The Virginia State Police is contacted for "GLINK" connection problems.
 - d. The Technical Services Sergeant or the City Information Technology Division is contacted for CAD/VCIN problems.
 - e. The Technical Services Sergeant (during normal business hours) or the City Information Technology Division is contacted for MDT problems.
- E. All sworn members and selected non-sworn members of the Department are granted access to the Department IBM Mid-Range Computer and the City Local Area Network (computer systems generally are hereafter called the "System")
 - 1. A member's level of access to various System programs is determined by his position assignment. Personnel requiring 24/7 access to records information are granted the appropriate access authority.
 - 2. The Technical Services Sergeant determines the member's level of access, and is the point of contact for all Department use of the System. The Technical Services Sergeant coordinates actions with the City Information Technology Department (hereafter known as "City IT") through the Police Systems Specialist assigned to the department by City IT.
 - 3. The City IT is responsible for all procurement, installation, repair and administration of the System, including all hardware and software, and arranges the member's initial access to the System.
 - 4. In the event that any part of the System is found to need repair, the member discovering the deficiency is responsible for notifying the Technical Services Sergeant, who coordinates repairs through City IT only.
- F. The use of the System is governed by Section 11.1 of the City Employee Handbook.

Effective Date: 07-21-2014	GENERAL ORDER	Number: 04-03
Subject: Computer Systems		Page: 3 of 5

- G. Members shall not attempt to gain access to parts of the System that they have not been granted access to. While a member may access the System from any Department computer, through the use of his individual password, every member's personally generated files are only available to the member himself (through use of his password), and the IT Department (for administrative / repair purposes).
- H. Members shall comply with state and federal laws regarding proper disposition of data retrieved from the System.
- I. Members are granted access to the Internet and the Intranet, for enhanced communication within and beyond the City.
 - 1. Members may send and receive electronic mail (hereafter called E-mail) through the Internet, from their issued laptop computers, personal computers, or mobile device for communication with sources outside the System.
 - 2. Members may send and receive E-mail from their issued laptop computers, personal computers, or mobile device for communication with sources within the System.
- J. Members shall understand and comply with copyright laws and specific license agreements of all City-owned or leased software which they use, and to which they have access.
- K. Members shall not give or sell a copy of City-owned or leased software to another person.
- L. Software that is not purchased or leased by the City shall not be loaded, copied or installed on any part of the System without prior written approval from City IT. Requests for the above actions are directed to the Technical Services Sergeant.
 - 1. In the event that the member has a need and justification to copy any City-owned or leased software for installation on the member's personally-owned computer, a written request for this action is forwarded to the Technical Services Sergeant, including a copy of the software license that states this practice is allowed.
 - 2. City IT is responsible for making a final decision on any such requests.
 - 3. The introduction of computer software and data disks into agency-controlled computer systems hardware is strictly prohibited.
- M. Members shall not make any changes to System configuration information, physically move a terminal, or connect a new terminal without prior approval from City IT.
- N. Members shall not add, delete, modify or copy any software installed in the System without the approval of City IT. Requests for the above actions are directed to the Technical Services Sergeant.
- O. Devices, equipment, or components of the System utilizing a location tracking feature shall not be altered, disconnected, disabled, or otherwise tampered with, unless approved by a supervisor.
- P. Members shall not store and/or duplicate any photographic digital information that is classified as evidence on any departmental or personal computer (system) without supervisory approval. Additionally, no digital photographs or video classified as evidence will be stored by and/or transmitted to other individuals without approval. No digital photographs or videos will be posted on the Internet without the approval of the Chief of Police or his designee.
- Q. Members shall not store personal photos on the City's server.
- R. No programs shall be downloaded from the Internet, or any other online source, and executed on the System, without prior permission in writing from City IT.
- S. Basic computer training is a part of the field training function. Additional computer training is offered periodically by City IT, either in-house or as provided by a contractor. Other training is available through the Academy.
- T. Members are reminded that data transmitted to and received via department owned computers is subject to release to the public under the Freedom of Information Act.
- U. Members' use of the computer regarding data transmitted must comply with General Order 2-1, Rules of Conduct.

Effective Date: 07-21-2014	GENERAL ORDER	Number: 04-03
Subject: Computer Systems		Page: 4 of 5

III. Mobile Computers

- A. Mobile computers are installed in most Department emergency vehicles as practicable, and select other Department vehicles. Mobile computers are connected to the System, and provide the following capabilities:
 1. Sending and receiving information.
 2. Make and receive routine inquiries from City, State and Federal sources.
 3. Receive supplemental information.
 4. Sending to and receiving messages from logged on users.
 5. Creating Police Reports and managing police calls for service
- B. The Technical Services Sergeant is the liaison and point of contact for all issues involving mobile computers. City IT is responsible for the procurement, installation, modification, maintenance and repair of mobile computers, sometimes using outside contractors.
- C. The Technical Services Sergeant and City IT have administrative access to the Mobile Data System.
- D. Mobile computer operation is governed by the "MDT Users Manual," published separately, as well as the provisions of this General Order.
- E. Mobile Data Terminal software is installed in all Department emergency vehicles, and selected other Department vehicles.
- F. Members shall not operate the mobile computer while simultaneously driving the vehicle.
- G. All mobile computer transmissions are digitally recorded and stored in the Department's Records Management System. The messages are only accessible to those members with administrative rights to the system.
- H. System access via mobile computers is controlled by individual passwords. The Police IT Specialist enters the member into the Mobile Data Terminal Server and sets a unique, individual password.
- I. All Mobile Data Terminals must remain physically locked while in the vehicle's computer docking station at all times. Members have the capability of removing the Mobile Data Terminals from the vehicle using a computer docking station key issued by the Public Safety IT Specialist.

IV. Electronic Communications System Audit

- A. The Technical Services Sergeant is responsible for performing quarterly audits of the various electronics communications subsystems utilized by department members.
- B. The purpose of this audit is to determine if members are using electronic communications devices in compliance with the provisions of the City's Employee Handbook and the department's General Orders.
- C. The audit's results are submitted to the Chief of Police who determines the investigating authority for any noted violations. The audit's results are distributed to the Command Staff.

V. Personal Computer Use

- A. Personal computers (hereafter called "PC's") are issued to sworn members of the rank of Sergeant and above, and to other sworn members according to job assignment. PC's are issued to selected non-sworn members according to job assignment. PC's are connected to the System.
 1. PC's may consist of laptop or desktop computers and related hardware and software.
- B. Members attend mandated computer training as directed and scheduled by City IT. Supervisors should ensure that members under their command attend additional, specialized computer training.
- C. The use of PC's is governed by Sections 11-1 and 11-2 of the City Employee Handbook, as well as the provisions of this General Order.

VI. Systems Security

- A. Members should consult with the Technical Services Sergeant or the Records Manager to ensure that the appropriate level of access is assigned, according to function, for files they are required access and for files that they create.
- B. Members are reminded that Department and individual user files are private and may contain confidential or sensitive information. As such all rights of privacy extend to computer files and files of another must not be viewed, copied, used, or altered without proper authority.

Effective Date: 07-21-2014	GENERAL ORDER	Number: 04-03
Subject: Computer Systems		Page: 5 of 5

- C. City IT uses a program to continually randomly check both network and individual user accounts for defensibility against security breaches. The Technical Services Sergeant is immediately notified by City IT of any account access or code breaches should they occur.
- D. The Technical Services Sergeant performs an annual audit of the System comprised of information obtained from City IT regarding security issues and ongoing password verification.
- E. Passwords, generally.
 - 1. All members are responsible for establishing personal passwords for access to the System according to guidelines established by City IT.
 - 2. Users are notified of a weak password that does not meet these criteria. Users are unable to change passwords until successfully complying with all of the above password creation guidelines.
 - 3. Members must change their password at least every 90 (ninety) days. If the password is not voluntarily changed, the software will force this change at the end of 90 days. Members may change their password at any time.
 - 4. Members shall not give their password(s) to anyone else, or allow anyone else to log on to the System using their personal information.
 - 5. In the event that the member is unable to recall his password or is otherwise unable to gain access to the System, he contacts the Police IT Specialist, or if after hours, contacts the City IT Help Desk and leaves a voicemail for assistance.
 - 6. City IT does not keep a record of individual passwords; however, City IT has administrative access to all parts of the System.

VII. Systems Backup and Storage

- A. Computer users have the option to store their data locally in their local folder on the computer's hard drive, or on other storage media or centrally on the network. Those users who store their data locally are responsible for performing data backups. Data stored centrally will be backed up nightly by City IT. The IT Department is not responsible for the loss of locally stored data.
- B. Network data is stored via a disk backup. The disk backup appliance is located at Fire Station 21 and accessible by authorized members of City IT.
- C. Local Data Storage is the responsibility of the individual user. Users are advised to recycle storage media whenever possible, or to destroy discarded media in such a way that data can no longer be retrieved.

Attachments: N/A

Index as: Computers
VCIN / NCIC
Computer Training
CAD
Password
Mobile Computer

References: N/A