5. COMPUTERS & TECHNOLOGY

(November 2007)

I. POLICY

To maximize the efficiency of members, and to enhance the quality of their work, the Department encourages its members to use computer systems and databases. In order to protect Department hardware, software, and the records stored in databases from unauthorized access and computer viruses, it is necessary for the Department to implement and enforce certain security measures and procedures. Relaxed security measures could result in severe damage to operating systems, data, software and hardware.

It is the policy of the Department that any and all information distributed in either hard copy or electronic forms is considered Departmental property. Unless specified otherwise, information stipulated as "For Official Use Only" shall not be distributed outside the Department without the written authorization of the originating division.

II. CHECKLIST (N/A) III. DEFINITIONS

Local Area Network: Also known as a "LAN**,**" it is a computer network limited to a specific group of computers enabling the sharing of information and resources.

Operating System: Also known as the "OS", it is the software that communicates with computer hardware on the most basic level. Without an operating system, no software programs can run. The OS is what allocates memory, processes tasks, accesses disks and peripherals, and serves as the user interface.

Server: Equipment that serves information to computers that connect to it. When users connect to a server, they can access programs, files, and other information from the server. Common servers are Web servers, mail servers, and file servers.

IV. FORMS (N/A) V. PROCEDURES

1. Electronic Mail System

General Responsibilities

Personnel staffing the receiving computers are responsible for the retrieval, printing, deletion and distribution of messages as appropriate.

Maintaining Integrity of Computer Systems

In order to maintain the integrity of interagency computer systems, prompt entry and cancellation of all appropriate information is imperative.

Employees are cautioned that e-mail is electronically recorded onto the LAN and is subject to both administrative review and the subpoena process.

Types of Messages

Each component is responsible for entering general announcements into the system such as births, deaths, etc.

E-mail shall not be used to send abusive, demeaning, harassing, or threatening messages.

Specific Responsibilities

- Telecommunications Section personnel shall receive messages to be entered into NCIC or MILES
- Fleet Management Section personnel shall transmit preventive maintenance notifications and other vehicle information
- Personnel Services Division employees shall enter transfer opportunities and promotional system notifications
- Offices of the Chief of Police and Assistant Chiefs shall enter administrative regulations and policies, promotional and transfer lists, and disciplinary actions

2. County-Owned Computer Equipment & Operations

(Administrative Procedure 119)

Only County-owned or acquired computer equipment will be maintained and operated within Departmental facilities, except the following:

- Personally owned portable units removed at the end of the tour of duty
- Computing equipment held as evidence
- Visitors using their own personal equipment
- Exceptions authorized by the Chief of Police or their designee

Local Area Network (LAN) computers will not be detached from the network at any time.

Absent Assistant Chief authority, employees are prohibited from making hardware repairs, software additions, or adjustments to County-owned computers.

Employees shall not attempt to modify any computer start up routine or operating system files.

Employees shall not password-protect the boot (start up) process of any County computer.

Employees shall not use County computer resources to produce personal material.

Absent the affected employee's expressed permission, employees shall not knowingly move, copy, encrypt, destroy, modify, delete or tamper with the electronic data files of other employees.

Employees shall not knowingly place a computer virus onto a County computer, onto the LAN, or in any manner deliberately abuse computer resources.

Except in cases of operational necessity, employees shall not divulge their network log-on password to others.

Computer resources are fixed assets and shall not be moved from the component to which they are assigned without Division Commander authority and notification of the move to the Technology Integration Section (TIS).

Annual Audit of System

Annually, the TIS will work with the County's Office of Information, Technology and Communications (OITC) to conduct an

audit of the central records computer system for verification of all passwords, access codes, or access violations.

Software

Only software purchased or acquired by the County will be operated on Departmental computers.

All software must be installed in accordance with United States copyright laws. Licenses for all division-specific software shall be maintained in a secure place within the Division.

Authorized personnel will remove all software that is not County-owned during service calls.

Software written by employees, using County computer resources, becomes the property of the County. This software shall not be copied, sold or transferred outside the Department without the consent of the Chief of Police.

Electronic Files

All files contained on Departmental hard drives, floppy disks or other storage media are considered work products. Therefore, employees should have no expectation of privacy regarding these files. Electronic files may be administratively accessed or monitored for various reasons, including, but not limited to, any of the following:

- System maintenance
- Internal investigations
- Subpoena process

All original case files, investigative files, notes, memoranda, letters, documents and other work products maintained on computer-readable media shall be stored within the District/Division generating the original file.

Files shall not be encrypted without the consent of the Commander/Director. In the event files are encrypted, both the unit OIC and Commander/Director shall be made aware of the encryption password.

Computer Removal

When a computer has been designated as non-serviceable or when a hard drive on a computer fails, the Department shall retain the hard drive for destruction.

In both cases, the Commander/Director shall contact the County's customer support center (Help Desk) to arrange for removal of the hard drive. A technician from the support center will respond and remove the hard drive. The Commander/Director shall document this removal on a memorandum. The memorandum and hard drive will be submitted to the Property Warehouse Unit (PWU) for destruction. When a computer is removed from service, the Commander/ Director shall contact the TIS for assistance with disposal. This step is crucial to ensure that the computer is removed from the Department's fixed asset inventory, along with the termination of all associated maintenance fees.

Removable Storage Media Destruction

When removable storage media (floppy disks, tape back up, etc.) containing confidential information or criminal history record information (CHRI) become unusable, employees will forward the media to the TIS for destruction.

Used Facsimile (fax) Machine Cartridges

When used fax machine cartridges are ready for disposal, they will be forwarded to the PWU for appropriate destruction. An interoffice memorandum from the Commander/Director shall accompany the cartridges. This memo may be sent directly to the PWU without going through the chain of command.

Commander/Director's Responsibilities

Each Commander/Director shall:

- Ensure the legality of all software installed on Departmental computers under their command
- Maintain all original software disks, documentation and licenses for software programs unique to their command
- Monitor the proper use of Internet access by employees
- Inspect Departmental computers each January and ensure the removal of any illegally installed software
- Forward a report to the TIS documenting computer inspection results each January
- Notify the TIS when computer resources are relocated within the division

Back-up Procedures

The OITC ensures that the Department's network files are backed up. A nightly incremental backup job is performed on servers from Monday through Thursday and a full backup is scheduled to run on Friday evening through the early hours on Monday morning.

The Exchange servers backup individual mailboxes for each storage group once a week starting at midnight. A full backup of all Exchange databases is scheduled to run every night.

The software and systems used in the backup process protect the County's data from hardware failures, errors, and unforeseen events by storing backup and archive copies off-line and in off-site storage facilities.

3. Computer-Assisted Dispatch Terminal (CAD)

Using CAD Terminals

CAD terminals shall be used for the following transmissions:

- Routine messages to other terminals
- Entering all calls for service received at Districts
- Entering working unit rosters
- Sending messages to the PSC for which the telephone is not required

Entering Line-Ups

Prior to field units beginning the watch, the unit rosters will be logged into a CAD terminal.

The following minimum information will be entered for each squad:

- Shift number, followed by sector designation letter, followed by the number 9 (i.e., 2A9) for the assistant officer-in-charge (OIC) (i.e., Senior Corporal)
- Sector designation letter, followed by the shift number, followed by the number 09 (i.e., A209) for the overlap assistant officer-in-charge (OIC) (i.e., Senior Corporal)
- Shift number, followed by the sector designation letter, followed by the number 10 (i.e., 3A10) for the OIC
- Sector designation letter, followed by the shift number, followed by the number 10 (i.e., A310) for the overlap OIC
- Squad number, followed by a letter for the shift commander (i.e., 51A)

- Call sign
- Officer ID number
- Beat assignments, if different from call sign
- Court or special assignments
- Leave

The system for assigning call signs to field personnel is:

- Shift number, followed by the sector designation letter, followed by the beat number (i.e., 1A2) for patrol units
- Sector designation letter, followed by shift number, followed by the beat number for overlap patrol units (i.e., A206)

Premise History Entry

When officers have legitimate reasons for requesting that an address or hundred block be entered as a premise history, the information should be made available to the dispatcher in the following manner:

- The officer desiring the premise history entry shall contact their supervisor and advise them of the reasons for the request
- If the supervisor approves, they shall direct a memorandum to the PSC supervisor requesting the entry

The request must contain the following information:

- The exact address of the problem and whether it should be entered as an exact address or hundred block
- The problem or potential problem
- The retention time desired (1-99 days). The information will automatically be removed from the computer at the expiration of the retention time
- The name, rank and assignment of the requesting supervisor

When the requesting supervisor feels that the information should be entered immediately, they may make the request by telephone followed by a written request. A telephone request shall only be entered for two days to allow for delivery of the written request.

Inquiries should be directed to the PSC supervisor.

4. Criminal Justice Information System (CJIS)

Informational Capabilities

The CJIS can be accessed via LANconnected computers. The system offers detailed information concerning the

personal and physical identity of defendants, prisoners and arresting officers, pending charges, bond arrangements and trial dates. To obtain user information, refer to current keystroke manuals. For operational inquiries, contact the Technical Services Division (TSD).

Dissemination of CJIS Information

Information obtained through CJIS is for official government use only. Secondary dissemination of information shall be limited to the following:

- Other government criminal justice agencies when mutual interests are involved
- As administrative and/or law enforcement responsibilities require

The disseminating employee shall ensure that the recipient identity is recorded by completing the "Log Transaction" entry when the data is retrieved from the terminal.

Maryland law prohibits secondary dissemination of CJIS information for other than official purposes. This restriction applies to motor vehicle and licensing information obtained through CJIS. Members shall direct requests for such information to the MVA. Any employee disseminating criminal history record information to unauthorized recipients is subject to:

- A maximum federal fine of $11,000 for each infraction
- Additional state-imposed sanctions

5. Office of Communications, Videotape Productions

The Office of Communications is responsible for:

- Coordinating production activities
- Directing/producing videos

Videotape Productions

Videotapes may be used to distribute information within and outside the Department. The Commander/Director originating the project and desiring to produce a tape for distribution will contact the Director, Office of Communications. The Director, Office of Communications, will determine whether the project is technically possible, and advise the requestor accordingly.

If the project is technically feasible, a meeting will be scheduled for the following individuals:

- Sponsor (usually a Commander or Director)
- Technical writer (researcher, expert, or individual with the required information)
- Producer/director (usually an individual from the Office of Communications)
- Creative writer (usually provided by the sponsor to write the script)
- Graphics representative (usually a graphic artist)
- Budgetary representative (usually from the Fiscal Affairs Division)

The agenda will be designed to determine program objectives, projected audience, production deadline, available talent and support, financial requirements, and other responsibilities.

Approval Authority

The Director, Office of Communications, or their designee, will review proposed programs. They shall approve or disapprove programs in consultation with the Chief of Police.

Production Responsibilities

The sponsor will provide:

- Production personnel
- Props and sets (other than that which is already available in the studio)
- Technical writer
- Scripts
- Responsibility for graphics and production costs will be determined at the preliminary meeting

VI. GOVERNING LEGISLATION & REFERENCE

This General Order addresses:

- Commission on Accreditation for Law Enforcement Agencies, Standards 17.5.1, 81.2.4, 82.1.6, 82.1.7, 82.1.8, 82.1.9

Governing Legislation:

- Code of Federal Regulations, Title 28, Chapter 1, Part 20
- Maryland Criminal Procedure, Title 10, Section 219
- Prince George's County Administrative Procedure 119