I. Purpose

This Directive defines the proper use of computer and information systems. These systems include desktop computers, laptop computers, PDA’s, servers, mobile data computers, electronic messaging (E-mail), data, software and Internet services, owned and/or maintained by the Maryland-National Capital Park Police, Montgomery County Division.

II. Policy

The Division is committed to providing an environment that encourages the use of computers and electronic information to support the Division’s activities. It is the responsibility of each employee to ensure that this technology is utilized in accordance with the Commission’s “Electronic Communication Policy”, for proper business purposes and in a manner that does not compromise the confidentiality of proprietary, protected, restricted or other sensitive information.

III. System Security and Maintenance

A. Each Division employee will execute a computer and information system policy statement (see Division’s Forms Log).

B. All completed policy statements will be maintained by Management and Technology.

C. If equipment needs to be serviced, repaired or programmed, contact the Research and Technology Help Desk.

D. The Records Management System (RMS) is maintained by the M-NCPPC Computer Services Division. The RMS System Manager (Park Police Records Supervisor) is responsible for the password system and setting access levels.

E. The Keystone CAD (Computer Aided Dispatching) and RMS are equipped with a 90 day password expiration system. This system requires all users to change passwords every 90 days. Maintenance and auditing of the password system are the responsibilities of the Division’s IT personnel. Documented audits of the full system will be conducted, at a minimum, on an annual basis.

IV. General System Usage

A. All computer systems, data and software owned, maintained or used by the Maryland-National Capital Park Police, Montgomery County Division are for official use only. No employee will use or cause to be used any computer system for personal gain or benefit of any kind.
B. No employee will install any personal, unapproved, or unauthorized software on any system owned or used by the Division or the Commission. **All disks and files must be checked for viruses prior to use.**

C. The Division reserves the right to monitor its computer systems and any data contained therein, at its discretion and to examine any system at any time.

V. Electronic Messaging / Internet Procedures

A. All electronic messaging / correspondence is the property of the Maryland-National Capital Park Police, Montgomery County Division.

B. Employees will not share an e-messaging password, provide e-messaging or make easily available any access information to an unauthorized user, or access another user’s e-mail box without authorization. **Employees must ensure they log-out of the e-mail system or secure computer terminal when not in use.**

C. Offensive, demeaning or disruptive messages are prohibited. This includes, but is not limited to, messages that are inconsistent with the Division’s and the M-NCPPC’s policies concerning “Equal Employment Opportunity” and “Sexual Harassment.”

D. Broadcast-type messages sent to all e-mail users outside the Division require prior approval by an employee who has supervisory authority.

E. The Division’s local area network (LAN) and the Commission’s wide area network (WAN), including connections to the Internet, are to be used for business-related purposes. Any unauthorized use of the Internet is strictly prohibited. Unauthorized use includes, but is not limited to: connecting, posting, or downloading pornographic material; engaging in computer “hacking” and other related activities; attempting to disable or compromise the security of information contained on Division computers.

F. Unless prior approval of management has been obtained, users may not establish Internet or other external network connections that could allow unauthorized persons to gain access to the Division’s computer systems or related information. Under no circumstances will information of a confidential or sensitive nature be placed on the Internet.

G. All files downloaded from the Internet must be checked for possible computer viruses.

H. Any employee who is found in violation of this policy will be subject to disciplinary action, up to and including termination of employment.

VI. Mobile Data Terminals

All officers with mobile data computers (MDC) will always be logged on to the PacketCluster system while on-duty, including part-time and overtime assignments. Officers will display their current status on the system.

A. Officers will not type messages while operating their vehicle.

B. **MDC talk messages are for official business only. Any other use is strictly forbidden.**
C. When making inquiries, officers will verify that the correct information is entered and examine all returns for accuracy prior to taking enforcement action.

D. Officers will always ensure that there is appropriate jurisdiction prior to taking enforcement action.

E. It is the responsibility of the officer receiving “possible hit” information (stolen/wanted record from the MILES or NCIC system) to review it in an expeditious manner and treat that information as they would a possible “hit” from a radio request.

   1. All potential “hits” must be given to the Communications Section by radio for confirmation.

   2. All stop information, requests for assistance, etc. associated with a mobile computer hit must be broadcast via radio.

   3. If an automatic hit notification is broadcast by PacketCluster and it is not a good hit, the officer making the initial inquiry must send an announcement message to all other MDC units in a timely manner.

Approved Park Police Document
Signed Original on File

End of Directive