DEPARTMENT INFORMATION SYSTEMS

FC No.: 1400
Date: 05-21-18

If a provision of a regulation, departmental directive, or rule conflicts with a provision of the contract, the contract prevails except where the contract provision conflicts with State law or the Police Collective Bargaining Law. (FOP Contract, Article 61)

Contents:

I. Policy

The police department will provide personnel with the information systems, services, and support necessary to perform professional, efficient, and cost effective public safety and law enforcement services. Information systems resource acquisition and distribution will be based on approved requirements, prioritized needs, and available funding resources.

II. Definitions

A. Department Information Systems: Any communications, radio, and data, hardware, software, and network support that is owned, operated, and maintained by the police department or for the department by the Montgomery County Department of ***Technology Services (DTS).***

B. Personal Information Systems: Any communications, radio and data hardware, software, or network support that is owned by a private individual, organization, or agency.

C. Internal Department Operations: Operational and administrative functions conducted to support the official business of the police department.

D. External Information Support: Hardware, software, and network links to provide department information to other agencies and or allow department access to information from other agencies to support department information needs. ***This includes "Cloud" based data systems which interface or integrate with Active Directory Services.***

E. Approved Requirement: A process initiated by a district or unit commander documenting a "need" for new or enhanced information systems. The need becomes an approved requirement when a solution is agreed upon and entered into the ***Information Management and*** Technology Division ***(IMTD)*** Acquisition Plan.

III. Acquisition of Hardware and Software

A. Establish and Validate a Requirement

Before new information system hardware**,** ~~or~~ software, ***or cloud-based solution*** can be acquired, the user must show a valid need. The need must be one that cannot be met by current department hardware or software. The district or unit commander will validate the need and forward a request to the ***IMTD Director***. The ***IMTD*** will plan an integrated solution with the user, provide a written reply, and enter the requirement into the acquisition plan.

B. Acquisition Plan

The acquisition plan is maintained by the ***IMTD*** and links multiple requirements to ensure the solutions are integrated and support department operations. The plan lists all validated requests for information hardware and software and tracks the requester and the funding status.

C. Funding

There are three primary sources of information systems funding: ***IMTD*** funds, department/unit funds, and grant funding. Most department information systems hardware and software will be purchased from ***IMTD*** funds. The funding levels, planning, and priorities are available for review in the acquisition plan. Units may fund information technology, but all acquisitions must be coordinated with the ***IMTD*** to ensure compatibility and standards are met. Grant requests for information systems hardware and software must be coordinated through the ***IMTD*** to insure compatibility.

D. Installation and Configuration

The ***IMTD*** will coordinate the installation and configuration of any information systems connected to the department or county networks. The ***IMTD*** will install and configure any stand-alone system when requested by the user.

IV. Repair and Maintenance

The ***IMTD*** Help ***Desk site*** http://mcphelpdesk.mcgov.org:8081 ***and telephone number (240) 773-5219***, are the users' link to all repair and maintenance problems. Users experiencing information system hardware or software problems must ***enter a ticket on the Help Desk site or*** call ***the Help Desk phone number*** for maintenance assistance. Only computers and associated equipment listed in the department's inventory will be serviced. Authorized outside contractors may be tasked by the ***IMTD*** or ***DTS*** to respond to equipment repair requests.

V. Inventory and Disposition of Hardware and Software

A. All computers, servers, and printers purchased by or donated to the department are entered in department inventory. This includes computer equipment purchased under grant programs, seized, or donated to the department. Inventory will be physically checked with divisions and units on an annual basis. An inventory tag ***or serial number is*** applied to each item. The information on this tag will be needed when requesting maintenance or repair. ***All subscription services are monitored for their usage and the number of licenses utilized.***

B. Information systems hardware is tracked by a database. ***Notification of IMTD*** is required before hardware is transferred within the department. Associated software is normally transferred with the hardware. The department information systems will only be run with licensed copies of software. All purchases of software must be coordinated with the ***IMTD*** prior to purchase to insure computability and ***DTS*** standards. Personal software must not be loaded or run on county information systems. Information systems equipment and software that no longer meets operational needs will be turned into the ***IMTD*** for proper disposition.

VI. Data Bases

The department ***currently maintains more than 40 servers that support various department information needs. Encompassed are virtual, physical and cloud-based data storage systems. All are secured and controlled by department staff via Active Directory and Microsoft services. New information processing requirements for new data resources must be coordinated with the IMTD. A department data inventory is maintained by IMTD to assist in development of information systems to serve unit or office needs. There are several information vehicles available for service, including "dashboards", SQL Server Reporting, and Crystal Reports.***

VII. Personal Information Systems

The use of Virtual Private Networks (VPNs) is encouraged for any personal devices. VPN accounts are issued by DTS and maintained by IMTD for access from remote locations and non-issued devices for secure transmission of data between devices. Department or other secured law enforcement information stored on a non-encrypted device is strictly prohibited.

VIII. Records Imaging System

A. The imaging system is in place to store copies of law enforcement information that is not recorded in E-Justice or the Maryland State Delta Plus system. The imaging system allows authorized users to view and print all department scanned information. All scanned information is the property of the Montgomery County Police Department. The Director, IMTD, is responsible for maintaining custody and ensuring the integrity and security of these records.

B. Records Section staff has been trained regarding the laws that govern the release of department records. Strict adherence to these laws decreases the department's risk of liability. With the exception of traffic collision reports, no reports should be disseminated by any employee other than the Records Section staff. All questions and requests for copies of reports should be referred to the Records Section at 240-773-5330.

C. The imaging system can be accessed via a link on the MCPD SharePoint Intranet site. Access must be authorized and a password is required. Contact the Information Management and Technology Division if there are any problems accessing this system. District PDSAs and PSAs have been trained on the system and can assist with any problems.

IX. Security of Computer Systems and Information

A. The Montgomery County Police Department has access to several computer systems (e.g., METERS, E-Justice, TRAQ, Delta Plus and LInX) and subscribes to various online subscription services (e.g., Entersect Police Online, Regional Pawn Data Sharing System, Auto Track, and Neustar's LEAP) that are personal information systems for external information support. These accounts are generally protected by an Active Directory logon ID and password which are required for access.

B. Employees are prohibited from providing the login or password information for any computer system or online subscription service to any unauthorized person including non-department employees. Employees will protect their logon IDs and password information to these accounts so that no unauthorized person can gain access to the information.

C. These data systems accounts, the results of queries, or the information obtained from these accounts may only be used for legitimate law enforcement purposes arising out of the employee's official, departmental duties. Secondary dissemination of the above information to unauthorized persons is strictly prohibited. Secondary dissemination is only permitted to authorized persons for legitimate, law enforcement purposes.

X. CALEA Standards: 11.4.4, 17.5.1, 26.1.1, 41.3.7, 82.1.1, 82.1.6

XI. Proponent Unit: Information Management and Technology Division

XII. Cancellation

This directive cancels Function Code 1400, dated 01-08-99, as well as Headquarters Memorandums 04-10 and 08-04.

J. Thomas Manger
Chief of Police