DEPARTMENT INFORMATION SYSTEMS

FC No.: 1400
Date: 12-30-20

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 Responsibilities

A. Establish and Validate a Requirement

Before new information system hardware, 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

Information systems are funded mainly by general funds and occasionally by grant funds. The funding levels, planning, and priorities for IMTD are set by the Police Chief with input from the Assistant Chiefs and the Director of IMTD. All information technology 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. ***Grant requests must include a review by the Department's Grant Manager.***

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 Procedures

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. ***IMTD may be contacted using the Help Desk ticket icon, located on your desktop computer, or by calling the Help Desk phone number, at (240) 773-5219.***

V. Inventory and Disposition of Hardware and Software

A. All ***information systems equipment to include communication devices,*** computers ***(desktops, laptops, tablets, smart devices)***, servers, and ***peripheral devices*** purchased by or donated to the department are entered in department inventory. This includes ***information systems*** 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. Databases

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

Employees are encouraged to use county approved collaborative document management and video conferencing systems such as SharePoint, Teams, and Power DMS when conducting County business on personal devices. Employees are responsible for updating and maintaining their security on their personal devices. Virus protection and keeping your operating systems/applications updated with the newest releases supports protection of the data systems and your personal device. 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. ***County employees who wish to obtain remote access may complete a teleworking application, via the e-portal.***

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 ***Custodian of Records, Deputy*** Director ***of*** IMTD ***Records***, 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 ***a*** logon ID and password ***(usually Active Directory), as well as, two-factor authentication methods*** which are required for access.

B. Employees are prohibited from providing the login ***ID*** 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, ***changing their password as necessary,*** 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, ***and must be logged, as system rules require, by the employee either electronically or written.***

X. Security Awareness Training

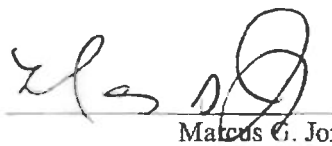
Each month, County employees will be enrolled in Security Awareness Training provided and managed by DTS. Compliance with the training helps to raise security awareness and foster secure behavior in handling and protecting County Information Technology systems and data. All County full-time/part-time employees, contractors, volunteers, and business partners with Active Directory user accounts and access to County IT resources are required to complete monthly security awareness training. Training will consist of the following:

1. ***Employees must complete the monthly security awareness training within the month assigned.***
2. ***The employer will allow time for the employee to complete their training.***
    - i. ***If an employee misses their training day, their supervisor will ensure the training is completed when they return to work.***
    - ii. ***Employees who are on extended leave will complete the mandatory security awareness training for the months in which they work.***
    - iii. ***Employees may choose to complete the work on their own time. Overtime compensation is not authorized.***
    - iv. ***Employees will receive automated reminders to complete their training, and suspension of computer access for non-compliance.***
3. ***Supervisors will monitor the employee's mandatory security awareness training.***
    - i. ***An employees' computer access may be suspended for non-compliance.***
    - ii. ***Supervisors and managers have access to an online tool to verify employee compliance via the department SharePoint site.***
    - iii. ***Prior to an employee's computer access being suspended, notification will be made to management and/or the employee's supervisor. If the employee is a member of a collective bargaining unit, notification will be in writing to their respective collective bargaining unit.***
    - iv. ***Discipline and/ or corrective actions for non-compliance will be progressive and follow the respective collective bargaining agreements and/or personnel regulations.***

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

XII. Proponent Unit: Information Management and Technology Division

XIII. Cancellation: ***This directive cancels Function Code 1400, dated 05-21-2018.***



Marcus G. Jones
Chief of Police