SECURITY AND PROTECTION OF INFORMATION

Directive: 11-103

Date of Issue: October 2014 Amends/Cancels:

I. PURPOSE

The purpose of this Directive is to provide guidance to members of DGS-MCP regarding the collection, storage, protection, and destruction of confidential personal information.

II. POLICY

It is the policy of DGS-MCP to conform with any provisions of state law or governmental procedures governing the Security and Protection of Information. All DGS-MCP employees will be responsible to follow reasonable security procedures for the handling, storage, and destruction of Personal Information and Sensitive Information, as defined hereinafter, collected from individuals during the normal course of business in all its forms - written , spoken, recorded electronically or printed. It is the intent of the agency that such Personal Information will be protected from accidental or unauthorized modification, destruction or disclosure throughout its life cycle.

III. DEFINITIONS

"DGS-MCP" includes all personnel with law enforcement-approved access to confidential information. This includes Police Officers, Police Communication Operators, Security Officers, and civilians assigned to Headquarters, Detachments, and the Security Card Processing Center.

"Personal Information" means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

- A Social Security number;
- A driver's license number, state identification card number, or other individual identification number issued by a unit;
- A passport number or other identification number issued by the United States government;
- An individual taxpayer identification number; or
- A financial or other account number, credit card number, or a debit card number that in combination with any required security code, access code, or password would permit access to an individual's account.

"Sensitive Information" means any information collected not classified as "Personal Information", but that contains an individual's name and any information about that individual that could reasonably be considered personal in nature. This includes medical information, criminal history

check, pre-employment background information, information about family members, credit history check, etc.

"Breach of the security system' means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by DGS-MCP.

IV. PROCEDURES

A. This directive applies to all personnel who have access to computer systems, networking systems, physical records (including electronic mail), peripheral equipment, workstations, personal computers (desktop and portables), within the Maryland Capitol Police. Network and computer resources include data, printouts, and telecommunications that permit access to records.

B. DGS-MCP prohibits any unauthorized access, disclosure, use, duplication, modification, diversion, destruction, storage, loss, misuse, or theft of (hard copy or electronic, this includes information captured as a record, or information. Any such unauthorized activities or misuse will be cause for disciplinary action to be taken to the fullest extent in accordance with DGS-MCP policies.

C. USERS

1. Users are expected to follow all policies and procedures related to records security and privacy of law records data in both physical and electronic format. All DGS-MCP personnel will comply with policies and procedures pertaining to the printing, copying and faxing of records. This includes transmission, viewing and distributing records.

2. All DGS-MCP personnel are expected to know and comply with all existing security and privacy policies. Only authorized DGS-MCP personnel will be given access to the communication infrastructure as it relates to records in a capacity limited to meet the ability to perform their duties appropriately.

3. All DGS-MCP personnel who have been determined to no longer need access to the communication infrastructure or specific areas of the network and applications will be removed from access lists, including terminated employees, employees on extended leave, retired or transferred employees with new duties and responsibilities.

D. COMMANDERS

Commanders are responsible for ensuring that records data privacy and information security measures are being followed for their areas. They are responsible for ensuring the records security and privacy of all department/agency data stored as either physical paper records or electronic records on departmental computer servers. They will work with the appropriate network and information security administration to ensure records security, and they must maintain a current working knowledge of Department policies pertaining to records security and privacy and identify necessary process improvements and/or changes when new policies are approved.

E. DOCUMENT STORAGE

1. The following procedures must be observed for storing confidential documents:

   a. All hardcopy confidential documents maintained by DGS-MCP shall be stored in a secured area accessible to only those employees whose job function requires them to handle such documents. A secured area includes a locked drawer, cabinet, or room. Access to these areas must be controlled and monitored.
   b. Any records to be destroyed will be destroyed in an appropriate manner as per the DGS-MCP records detention policy. All personnel must prevent the improper disposal or destruction of records that may directly or indirectly breach records confidentiality.

F. DOCUMENT SAFEGUARDING

1. Operational needs within DGS-MCP frequently require confidential documents be removed from secured areas in order to perform necessary job functions. The following procedures shall be followed when such documents are in possession of an employee in the course of his/her job duty.

   a. When not in a secured area, the confidential documents must not leave the employee's immediate control. Documents of this nature cannot be left unsupervised while physical controls are not in place.
   b. When not in a secured area, precautions must be taken to obscure the confidential information from view, such as by means of a file folder or envelope. Confidential information shall not be left in plain view in a vehicle.
   c. All files containing confidential documents must be inspected thoroughly to ensure they do not contain any misfiled confidential information from other files.
   d. To protect electronic confidential documents, all employees shall leave their computers in a 'locked or 'logged off' state when not in immediate vicinity of his/her work area.

G. RECORDS RETENTION

1) Any unit, division, sections, or detachment with the responsibility for managing forms, files, records, documents, or information will strictly adhere to the guidelines set forth in the records management directive 11-101 (Filing and Retention Schedule).

2) The preferred method for destroying printed, files, records, documents, or information will be by using a device capable of shredding paper in such a manner that it cannot be retrieved or reconstructed.

3) When shredding records of an individual that contain personal information DGS-MCP shall take reasonable steps to protect against unauthorized access to or use of the personal information, taking into account:

   a) Sensitivity of the records;
   b) The nature of the unit and its operations;
   c) The costs and benefits of different destruction methods; and

d) Available technology

H. INFORMATION SECURITY

1) The operating system(s) used by DGS-MCP to manage and operate the Access Control Program are located on a separate stand-alone network (security. Local). The network is closed to all outside influences and may only be accessed by those granted with administrative rights by the Chief of Police.

2) Methods of access will be by a unique user name and password for identifying the user and tracking the user's access to the system.

3) All servers and storage devices are in a secured facility accessible only by authorized personnel. Both areas are climate controlled with fire suppression systems and uninterrupted power sources.

4) In the event of a power outage all servers and storage devices have been outfitted with one hour battery backups that automatically engage until overridden by the generator.

   a. The generators are powered by natural gas and will run indefinitely as long as the gas supply is not interrupted.

5) When a member of DGS-MCP with administrative rights is transferred, resigns, retires or is terminated their change in work status is immediately forwarded to the Commander of the Support Services Unit. The Support Services Unit is responsible for managing the Security Card Processing Center and the DGS-MCP Information Technology Unit. An employee with administrator rights will immediately remove that right from the employee in question.

6) DGS-MCP will maintain a management practice for information systems to include regular patching and updates made to operating systems and individual applications.

   a. As a result of the system being housed as a standalone network updates and patching are provided by the vendor and installed manually by a DGS-MCP Systems Administrator.

7) DGS-MCP will maintain a backup security plan in the event access control systems, surveillance devices, and/or systems that manage information that are rendered inoperable.

   a. In the event the proximity system used to control access and/or the security cameras are rendered inoperable current Standard Operating Procedures dictate the following.

      1) All exterior doors will be manually secured by lock and key.

      2) Exterior doors that cannot be secured by lock and key will be chained and padlocked.

3) Law enforcement/security staff may be detailed to any security post affected until the systems are restored.

4) Law enforcement/security staff will increase exterior perimeter foot patrols until the systems are restored.

I. INFORMATION SECURITY BREACH

1) In the event of a breach of security resulting in the loss or potential loss of individual's personal information DGS-MCP will immediately conduct an investigation to determine whether the unauthorized acquisition of the information has been misused.

2) DGS-MCP will notify the Office of the Attorney General (OAG) for DGS.

3) If the breach of security was from a security system DGS-MCP will notify the DGS Information Technology Group.

4) On the advice of council DGS-MCP may be asked to notify any or all individual's affected by the breach

J. VERBAL SECURITY BREACHES

DGS-MCP personnel who have access to records shall only communicate sensitive information to appropriate personnel. When an employee is in doubt regarding the lawfulness or appropriateness of the information release, then they should not release the information. The employee shall immediately contact a supervisor who shall determine if the information is to be released.

K. RESPONSIBILITY

1. All members of the department shall know and comply with all aspects of this Directive.

2. All commanders and supervisory personnel are responsible for ensuring compliance with the provisions and intent of this Directive.