GAITHERSBURG POLICE DEPARTMENT			
Department Computer and Network Security			
GENERAL ORDER	108.7	Related CALEA Standards: 41.3.7, 45.2.1, 53.2.1, 82.1.6, 82.1.7, 82.1.8	
Effective Date	08/16/2017		
Authorized by:	Mark P. Sroka CHIEF OF POLICE	SIGNATURE Mark Sroka	DATE 08/16/2017

I. PURPOSE

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.

II. POLICY

The Department encourages its members to use computer systems and databases to maximize efficiency and enhance the quality of their work. Inadequate security measures and computer viruses can result in loss or damage to data, software, and/or hardware. To ensure that Department computer systems are performing properly, and the integrity of the records, files and data contained therein are not compromised, the Department coordinates with the City's Information Technology Department to monitor computer and network security.

III. DEFINITIONS

A. Information Technology Resources

Within the context of this directive, the term "information technology resources" includes any portion of technology owned, used or controlled by the City, Montgomery County or the State of Maryland. These include, but are not limited to desktop and laptop computers, mobile data terminals, servers, networks, related equipment and software applications, supporting systems and the data transmitted or stored on those systems, Internet services, Intranet services, telephones, voice mail, electronic mail (email), facsimile machines, photocopiers, printers, speed camera systems, License Plate Reader (LPR) systems, NCIC/CJIS terminals, CAD terminals, In-car camera systems, Body Worn Camera (BWC) Systems, Mobile Automated Fingerprint Identification System (AFIS), and Department issued computer media storage devices.

B. Public Records

Within the context of this directive, the term "public records" includes, by law, all official books, papers, or records whether kept on a manual or automated basis, which are created, received, or used by the State or any agency thereof, a bi-county or multi-county agency, any county, municipality, or other political subdivision.

IV. PROCEDURE

A. General Provisions

1. In accordance with policy outlined in the City's Personnel Rules and Regulations Manual, hardware and software installations and upgrades to City equipment shall only be done by authorized personnel from the City's Information Technology (IT) Department, or the Police Systems Support Manager with authorization from the City's IT Department..

2. Before purchasing or obtaining equipment and/or software for use in conjunction with information technology resources, the Information Technology Department must be:

   a. Contacted regarding the proper licensing of software; and

   b. Contacted to confirm the capability with the City's existing information technology resources.

3. The City's Information Technology Department personnel monitor information technology resources, on a continual basis and through the use of automated systems, to detect:

   a. Security breaches, privilege escalation, or information technology resource access violation; and

   b. Prohibited activities outlined in the City's Personnel Rules and regulations Manual.

4. Information technology resources will not be left unattended while logged on to the City, Montgomery County, or State of Maryland network, or any password protected system. Users shall lock the information technology resource or log off if the need arises to leave the information technology resource.

B. Audits

1. The purposes for auditing Department computer~~s~~ systems are to ensure data security, system integrity and efficiency.

2. Computer systems and databases maintained by the City are audited by the City's Information Technology Department, on a continual basis, through the use of automated systems for verifying

user accounts, passwords and access security.

3. A complete audit of user accounts, passwords and access to police data resources is conducted, at least annually by the City's Information Technology Department, and a report is forwarded to the Accreditation Manager.

4. Audits of NCIC and CJIS terminal use are conducted, on an annual basis, by the Maryland State Police and the Maryland Department of Public Safety and Correctional Services, to ensure the integrity of criminal history records information and proper use of these resources.

5. As a participating member of the LInX program, an annual audit is required that consists of reviewing the agency's LInX access, usage, training, security, and other related information sharing policies to ensure they are up to date and comprehensive and will protect the data of all agencies in the LInX system.

C. <u>Password Protection</u>

1. To protect information technology resources from unauthorized use, access to all desktop and laptop computers and mobile data terminals require username and password authentication.

2. Department personnel will only enter those usernames and passwords for which they possess the authorization to use, for accessing City, County, State and national computer systems and resources.

3. Passwords and access codes are confidential and will not be disclosed to others, including those members of the Department who also have authorized access. Accountability for systems use is associated with the user logged on at the time.

4. Pursuant to the provisions of CR 8-606 it is unlawful for a person, except under proper authority, to do or attempt to willfully:

    a. Make a false entry in any public records; and/or

    b. Alter, deface, destroy, remove, or conceal any public records; and/or

    c. Intentionally access public records for other than official purposes.

5. Pursuant to statute, a person may not intentionally, willfully, and

without authorization access, attempt to access, or cause access to a computer, computer network, computer software, computer control language, computer system, computer services, computer data base, or any part of these systems or services to alter, damage, or destroy data or a computer program stored, maintained, or produced therein, or any part of these systems or services.

6. A person may not intentionally, willfully and without authorization, identify or attempt to identify any valid access codes, or to distribute or publicize any valid access codes to any unauthorized person.

D. <u>Releasing Information</u>

1. The information contained in Department information technology resources, is for official use only, by authorized Department personnel.

2. Information from Department information technology resources may be released to members of other law enforcement agencies for official purposes, but shall not be released or disclosed to members of the public or the media.

3. Statistics and statistical information may be used by Department members when meeting with citizens and citizen groups in order to address community concerns, perceptions or misperceptions of crime.

4. Personnel using statistics and statistical information must be cognizant of the fact that they are dealing with raw numbers (basically calls for service) and not properly analyzed data.

5. Personnel shall not use in meetings with citizens or citizen groups, or make available to non-law enforcement personnel, information contained in crime analysis reports or the reports themselves if the information is confidential or not otherwise considered to be within the public domain.

6. Information must be carefully screened before being discussed with non-law enforcement personnel, because:

   a. The information that forms the basis for a crime analysis report frequently names suspects or persons who have not been charged in connection with any of the listed incidents; and

   b. May name juveniles who either have or have not been charged with a delinquent act.

E. **System Back-Up Schedule**

1. All Department data stored on the file server is backed up on a regular schedule by the City's Information Technology Department.