Lexington Police Department

Lexington, Kentucky

GENERAL ORDER

BY THE AUTHORITY OF THE CHIEF OF POLICE

G.O. 2015-06A **Computer Policy**

Rescinds: GO 2015-06

References: CALEA Chapter(s)

Effective Date: 12/02/16

Distribution: All Department Employees and Volunteers

Originally Issued: 1999

I. PURPOSE

The purpose of this policy is to outline the use and maintenance of the department's computers and network, including mobile data computers (MDC's). This policy also outlines department procedures related to AS/400 security and for data storage and disposal.

II. POLICY

It shall be the policy of the Lexington Police Department to maintain computer technology that allows efficient delivery of law enforcement services, and to operate the equipment in a professional manner. Computers, including MDC's, shall be utilized in accordance with applicable sections of GP 25 "LFUCG Computer Policy", the FBI Criminal Justice Information Services [CJIS] Security Policy and the requirements set forth in the training guidelines from the Department of Criminal Justice Training and the Kentucky State Police. All department employees are expected to abide by applicable sections of GP 25 and the FBI CJIS Security Policy in their use of department owned or maintained computers and associated hardware and software.

It shall also be the policy of the department to use computer software in accordance with all applicable statutes and in accordance with requirements established by software publishers in licensing agreements governing the permitted use of that software.

It shall also be the policy of the Computer Information Systems Unit (CIS) to perform proper backup procedures of locally stored data on the AS/400, Mobile Data Servers and Digital Evidence Server. CIS shall also be responsible for the proper disposal of any outdated or unusable backup or long-term storage media.

III. DEFINITIONS

Computer Hardware: includes the laptop, tablet, desktop or server computer components, peripherals, monitor, printer, wiring, and associated parts that are the property of the department.

Computer Software: the operating system and approved programs that function within the computer.

Computer Technician: technicians assigned to the Computer Information Systems Unit (CIS).

Mobile Data Computer (MDC): Any computer normally utilized in the vehicle for the purpose of accessing wireless resources within the department.

Network: a computer information system that links multiple computers for the purpose of sharing information. The term network in this policy applies to all local area networks (LAN), wide area networks (WAN) and wireless networks within the department.

IV. COMPUTER PURCHASES

A. Specifications for hardware and software:

1. The specifications for computer hardware and software purchases shall be forwarded to the Computer Information Systems (CIS) Unit for approval.

2. Specification evaluation will determine if standard equipment and software have been included in the order, purchase price is appropriate, and that contract vendors were utilized.

B. No personally owned computer hardware or software may be purchased or used on the department network without prior approval of the CIS.

V. COMPUTER MAINTENANCE AND REPAIR/WORK REQUESTS

A. All requests for computer support or repair shall be made to the CIS Help Desk. The email address for the Help Desk is CISHelpDesk@lexingtonpolice.ky.gov. Unauthorized employees or other personnel should not attempt repairs to microcomputers.

B. Only authorized computer technicians are permitted to make computer repairs, modifications, and to remove or install parts.

C. Department employees designated by CIS will also be permitted to make computer repairs, modifications, and to remove or install parts.

D. No desktop computers, monitors, scanners, printers, docking stations or associated peripherals are to be moved without the permission of CIS.

E. Semi-rugged laptops and/or MDC's issued as a desktop replacement must remain with the assigned bureau and are not to be moved upon user transfer.

F. Damage to any computer or associated equipment must be reported to CIS immediately.

G. Potential threats to network security including viruses, malware, or network security breaches must be reported to CIS immediately.

VI. COMPUTER SOFTWARE USE (PRIOR APPROVAL)

A. Computer software that is not part of the standard operating package shall be approved by CIS prior to purchase and/or installation. This will ensure compatibility with the operating system, server, and other systems in use.

B. Computer software upgrades shall be budgeted by each bureau.

C. Computer software that utilizes games shall not be installed in any department computer. If game software arrives preinstalled on a computer, the bureau receiving the equipment shall arrange to have the game software removed by contacting CIS.

D. Department employees shall not download software from the Internet without prior approval from CIS.

E. Prior to installation of any software package, the employee authorized to conduct the installation shall complete a virus scan.

F. Media that do not originate from within the department or government shall have a virus scan performed before any files are accessed on the media. This requirement also applies to files transferred to or from private computers, such as work performed on a personal home computer.

G. Virus scans are recommended for all media, regardless of origin, prior to accessing files in order to protect the department's computer network.

H. Only CIS will conduct software installation on the network server and computers.

VII. NETWORK AND SERVER MANAGEMENT BY COMPUTER TECHNICIANS

A. Only computer technicians or a CIS designee shall perform installation and maintenance of computer network connections.

B. Only computer technicians or a CIS designee are authorized to access network management applications on the department's network servers.

C. Requests for and establishment of shared directories on the network system shall be coordinated through CIS.

D. Requests for activation of network and email accounts shall be forwarded to CIS for creation. Account requests must include the user's full name (including middle initial), employee number (if applicable), anticipated start date and network access needed. It is preferred that the request be sent to CISHelpDesk@lexingtonpolice.ky.gov.

VIII. INTERNET AND NETWORK USE AND/OR ABUSE

A. Department employees shall not intentionally access any web site that contains pornographic images or messages unless required by job assignment or investigative function.

B. Users are expected to use Internet access for business related purposes for the Department of Public Safety. Incidental use is permitted, provided that such use does not interfere with the performance of the user's duties and does not affect the security and performance of the police network system. Excessive non-business usage may result in disciplinary steps being taken.

C. Department employees shall not image, copy, distribute, store, display, or cause to display

on their desktop, laptop, or MDC computer any pornographic or otherwise offensive image or message.

D. Department employees shall not download any software to any department computer or computer device without prior approval of and scanning by a computer technician.

E. Employees are not authorized to access games on the Internet.

F. Employees shall not attempt to access data and/or files within any department or Urban County Government computer system that they have not been specifically authorized to access. Files include, but are not limited to, personnel records databases, juvenile databases, the home directory of individual users, and other files with limited clientele authorization.

G. Disciplinary charges may be initiated against any department employee who intentionally accesses or attempts to access any computer file, directory, or database that they are not specifically authorized to access or for which prior authorization may have existed, but was subsequently removed.

H. Department employees shall not attempt to circumvent computer security features designed to provide privacy (e.g. utilizing another's password to gain access, "hacking", bypassing security features, etc.).

I. The addition and removal of authorized users from shared computer files shall be performed by a computer technician. Bureau assistant chiefs or designees shall notify a computer technician when employee transfers necessitate the addition or removal of access rights for an employee.

J. Computer technicians are authorized to access all computer directories for the purposes of computer network maintenance, programming, and transfer of data between server drives.

K. Computer technicians are authorized to delete any game file located on any department computer and/or any program that is causing computer network trouble.

L. Computer technicians are authorized to remove any audio or video file located on any department computer or network drive when that file is for entertainment purposes only.

IX. EMAIL USAGE

A. The default size for Exchange mailboxes is 2GB of total storage (Inbox, Sent Items, Calendar, Contacts, Deleted Items, etc.). Users are encouraged to delete items no longer needed and to store long-term items in Outlook personal folders.

B. Email is not actively monitored, but no privacy is guaranteed. CIS reserves the right to open and read mail and to make stored communications available to third parties when any of the following conditions exist:

1. When opening and reading mail is required to maintain or protect the integrity

and/or operation ability of the public safety network or other computing resources.

2. When such action is required in order to comply with a court order or to comply with any applicable local, state or federal statute.

3. When such action is required pursuant to an internal investigation.

4. When such action is required in order to comply with an open records request.

5. Upon specific granted permission from both the sending and receiving parties.

C. Electronic mail and all mailbox components are recorded as part of the police data backup system and may be subject to records retention requirements.

D. Use of email is subject to, but not limited to, the following restrictions:

1. Electronic mail is provided for use by employees in the performance of their duties. However, incidental use is permitted, provided that such use does not interfere with the performance of the user's duties, does not affect the security of the police network system, and does not affect the performance of the network or mail system.

2. Attachments to unsolicited mail should not be opened or saved.

3. Signature lines must be kept appropriate for business use. Advertisements are prohibited. Signatures using graphics must be limited in size to 25kb.

4. Email backgrounds are not to be used.

E. Suspicious emails received should not be opened. The sender's address should be reported to CISHelpDesk@lexingtonpolice.ky.gov.

X. ELECTRONIC DATA

A. All user data files are to be stored on network drives. Data stored on computer local drives (C, D, etc.) will not be backed up by CIS and may be deleted or lost.

B. All data stored on media owned by the department is the property of the department.

C. All users who access data owned by the department shall take all necessary and reasonable measures to protect that data from loss.

D. No user shall make copies of data owned by the department for personal use or for any purpose not required by his or her assigned duties.

E. Disclosure of data to persons or agencies outside of the department is limited to any of the following conditions:

1. The other party is acting as an agent for LFUCG (legal counsel, insurance company,

etc.).

2. The data is required by a government or police agency.

3. The request was made as an open records request and was approved by the Department of Law or its designee.

4. A separate policy, memorandum of agreement or memorandum of understanding exists that expressly authorizes the release of the requested data.

5. Release of the data was approved by the Chief of Police or designee.

XI. USER SECURITY

A. User login credentials must be used only by the employee or volunteer they are assigned to and not shared with others.

B. Passwords are to be kept secure and confidential.

C. Any suspected loss of password information must be brought to the immediate attention of CIS.

D. CIS shall conduct annual audits of all employees, volunteers and other personnel accessing the department network and data, including but not limited to: Active Directory, Microsoft Exchange, AS/400, E-Warrants, Mobile Data Software, KyOPS and CourtNet.

1. Annual audits facilitate establishing and ensuring the security and system integrity of the AS/400 and department network.

2. Any detected breach of security measures will be documented and forwarded to the CIS lieutenant.

XII. CONSIDERATIONS FOR UTILIZING MOBILE DATA COMPUTERS

A. No employee or volunteer shall operate a mobile data computer without first receiving the required training from CIS and/or the Training Section. This training shall include an orientation course as well as LINK/NCIC training if the employee or volunteer has not already previously attended this training.

B. All issued computers, power cords, printers, and scanners shall be assigned to the employee or volunteer by CIS as issued equipment and will be maintained as an inventoried item. Docking stations and modems shall be considered part of the equipment assigned to the vehicle.

C. The security and proper use of the MDC is the responsibility of the employee or volunteer who is issued the equipment. All necessary precautions must be taken to ensure the integrity of the computer network.

1. While the vehicle is not in use, the MDC shall be secured in the employee's or volunteer's home or in the vehicle trunk. Leaving the unit in the vehicle can subject it to extreme temperatures, which can degrade the life of the equipment. An unattended MDC may also be the target of a theft, resulting in the loss of the MDC and damage to the vehicle incurred during the commission of the theft.

2. An employee must lock their vehicle upon exiting if they are going to be out of sight distance of the vehicle while the MDC is in a "logged-on" status.

3. No computer software or files of any type may be introduced into the MDC unless they are issued from or approved by CIS.

D. Any problems with the MDC network shall be immediately brought to the attention of CIS regardless of the time of day to minimize the possible impact on other users.

E. All LINK/NCIC transactions shall adhere to the procedures outlined in current policies.

F. Hit confirmations for all transactions (LINK/NCIC and warrants) will be confirmed by E911. No enforcement action will occur solely as the result of an MDC hit, with the exception of an e-warrant hit.

G. Playing games of any kind on the MDC is strictly prohibited.

H. While it is understood that the employees operating their vehicles may need to touch a button or the screen display to reply to a dispatched call, they are strongly discouraged from attempting to type or enter any information into the MDC while the vehicle is in motion. Additionally, employees should refrain from attempting to read information on the MDC while the vehicle is in motion.

XIII. MDC UPDATES

A. MDC updates fall into two categories: Computer Information Systems Unit updates and employee updates. These updates are required by all MDC users, regardless of assignment.

B. Computer Information Systems Unit updates will occur as needed and will be coordinated by CIS. When instructed, employees must bring their MDC in for update at their scheduled times.

C. Field Updates are those updates initiated by the user.

1. The first type of update is the General Update, which is completed using the "Update MDC" link on the employee's desktop. This update must be completed at least once per week.

2. The second type of update is the AVG Anti-Virus update. This update will normally occur automatically. In the event that the update fails, the employee will complete the AVG update manually. This update must be completed at least once per month.

3. The third type of update is the general KyOPS update. This update will be either a code files update or a program update. The employee will be prompted for these updates when they transmit in KyOPS. This update must be completed within two weeks of the systems prompt for update or as directed by the KyOPS Administrator.

4. The fourth type of update is the KyOPS Map Files update. This update is accessed in the Help menu in KyOPS. This update must be completed every six months, or as directed by the KyOPS Administrator.

XIV. PROCEDURES FOR DATA STORAGE AND DISPOSAL

A. CIS is responsible to establish and maintain procedures for saving all work products of the department that are stored for the purpose of data sharing and retrieval.

B. CIS is responsible to maintain and monitor automated backup of department servers.

1. Data backed up to hard drive storage will be redundantly stored at an off-site location.

2. Data backed up to tape (AS/400 and Message Switch) will be stored off site.

C. All backup or long-term storage media that is no longer usable will be disposed of in the following manner:

1. Digital media (i.e. tape/diskette/compact disks/hard drives/etc.) will be securely stored in the Computer Information Systems Unit Network office prior to destruction.

2. All tape and diskette media is to be magnetized with a commercial magnet to ensure data scrambling.

3. All hard drive media is to be formatted.

4. All media shall also be disassembled (i.e., cases broken, compact disks broken, tape taken from the reel, drive logic board removed, hard disk platters removed from case and drilled) prior to disposal to discourage attempts for retrieval.

XV. ELECTRONIC DATA STORAGE BY SERVICE PROVIDER

A. If the agency uses a service provider for electronic data storage, a written agreement is established addressing:

1. Data ownership;

2. Data sharing, access and security;

3. Loss of data, irregularities and recovery;

4. Data retention and redundancy;

5. Required reports, if any; and

6. Special logistical requirements and financial arrangements.