KANSAS CITY MISSOURI POLICE DEPARTMENT **PERSONNEL POLICY**	DATE OF ISSUE 9/16/2021	EFFECTIVE DATE 9/16/2021	NO. 260-1

SUBJECT

Policy Series 200: Employee Guidelines
260 - Computer Use and Security

AMENDS

REFERENCE

RSMo. 569.094; 569.095; 569.097; and 569.099
Personnel Policy 330, "Department-Owned Equipment-Privacy and Security"
Patrol Bureau Memorandum 20-03, "GPS Receiver in Department Vehicles"

RESCINDS

PPBM 260

I. INTRODUCTION

The security of the Kansas City Missouri Police Department's (Department) computer system is of paramount importance. Users will strictly adhere to the following guidelines on the usage of Department computers and associated software to ensure compliance with federal copyright laws and protection against computer viruses. This policy provides instructions for members regarding computer systems, electronic mail (e-mail), and Internet usage.

II. TERMINOLOGY

A. **Breach -** A break in the system security that results in admittance of an unauthorized person or program to a Department computer system.

*B. **Bring Your Own Device (BYOD) –** Privately owned personal computer equipment such as desktops, laptops, IPads, cellphones, or tablets.

C. **Electronic Mail (E-mail)** - A system for sending and receiving messages electronically over a computer network accessed through a Department owned computer.

*D. **Encryption –** The process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. Encryption will be Federal Information Processing Standard 140-2 certified for any Criminal Justice Agency.

E. **Firewall** - A system (hardware or software) designed to prevent unauthorized access to or from a private network.

*F. **Hardware** - The physical computer system or any physical part or mechanism used as an integral or peripheral component of a computer system, e.g., telephone, memory modules, display monitor and interface card.

*G. **Help Desk -** A resource intended to provide the end user with support. The purpose of a help desk is usually to troubleshoot problems or provide guidance about products such as computers, peripherals and software.

H. **Intranet -** Uses Internet based technologies within an organization to facilitate communication and provide integrated access to information.

I. **Internet -** A worldwide network of computers linked together by various communication systems including local telephone services.

*J. **Network -** A system of computers, printers, and storage devices linked by direct connection, over data circuits, fiber optic lines or via other electronic transmission methods that allows shared access to all resources on the network.

1. Home Directory (H Drive) – A personal drive on the Department's network that only the member can access for their Department documents.

2. Information Drive (I Drive) – The Department resource drive. All members have access to this drive.

3. Public Drive (P Drive) – The drive where members can temporarily share documents between each other, other sections and units.

4. Shared Drive (S Drive) – The drive members can access to share Department documents between their section or unit.

K. **Malware -** Short for "malicious software," malware refers to software programs designed to interfere with normal computer functions or sends personal data about the user to unauthorized parties over the Internet.

L. **Microsoft Outlook -** A software application used to create, receive, transmit, store, and archive E-mail messages as well as store calendar, tasks and contact information.

*M. **Source One –** A data archiving program that enables the Department to efficiently capture, index, store, manage and retrieve all data.

*N. **Software -** The programming instructions the computer executes to perform tasks. All software must be approved and purchased by the Department.

1. **Shareware Software -** Software obtained through public sources with normally limited features, periodic visual reminders to purchase, or a time limit cutoff to prevent use without purchase.

2. **Open Source Software** - Computer software whose source code is available under a license or arrangement such as the public domain that permits users to use, change, and improve the software, and to redistribute it in modified or unmodified form.

O. **Unauthorized Equipment** – Equipment that has not been approved and provided by the Department or is not properly licensed to the Department.

P. **Unauthorized Software** – Software that has not been approved and provided by the Department or is not properly licensed to the Department.

Q. **Virtual Private Network (VPN)** - A private communications network often used by companies or organizations to communicate confidentially over a public network.

III. POLICY

*A. These procedures apply to all members of the Department utilizing Department computer equipment or Department computer systems, to include computer equipment in Department vehicles. Use of these systems implies that members agree to comply with all applicable policies, guidelines and laws regarding their use.

*B. Unauthorized members will not unplug or alter computer equipment inside a police vehicle.

C. Only members of the Information Services Division (ISD) will install hardware/software on Department computers.

*D. ISD is the central location for storage and historical reference for the following technology, including but not limited to:

1. Computer programs and software

2. Internal and external servers

3. Applications

4. Platforms

5. Support systems

E. ISD is responsible for granting and monitoring access to Department computer systems by issuing each Department member a User ID. Members are prohibited from using any User ID which is assigned to another person. Members needing assistance acquiring a User ID and/or password are directed to contact the Help Desk.

*F. All units or members, which are presently using computer programs, applications, software, or platforms unique to their element (not typically used Department wide), will forward program information to the ISD, to include the below information:

1. Program name and date of initiation.

2. Type of program, e.g., open, closed, code involved, developer, etc.

3. Name and phone number of developer or owner of property rights.

4. Brief synopsis of the program and its intended uses.

G. Members are responsible for access to and use of their User ID and password. Members are responsible for logging off the network upon completion of their computer activity or locking their workstation.

*H. Members will not disseminate or disclose log-in or user ID information, Department network security details, or other confidential information outside the organization.

I. Members will not alter or copy a file belonging to another user unless they need to access those files in the performance of their duties.

J. Members will not use the Department computer systems to invade the privacy of other Department members by unnecessarily reviewing their files and e-mail.

K. Members will not interfere with or disrupt any Department computer system, internet user, program, or equipment. Disruptions include but are not limited to propagation of computer worms, viruses, or other debilitating programs, and using the Department computer system to make unauthorized entry to any other machine accessible via the computer system or internet.

L. Each member is responsible for taking reasonable precautions to avoid introducing viruses, worms and malware to Department computer systems.

1. Members will notify the Help Desk if a virus has been introduced to the network.

*2. Members will use caution when using flash drives from outside sources/entitles (e.g., conferences or vendors) and will contact the Help Desk with any concerns.

*M. Files saved to the Public Drive (P:\Public Drive) on the network should be backed up by the end user. Anyone on the network has access to that drive and has the ability to delete the files located on that drive. The files will be deleted after 30 days and are not part of the network wide backup.

N. No unauthorized equipment or data will be attached to the network.

*O. The Department reserves the right to access, view and copy any user's electronic communications messages, files, data, correspondence, log files, etc., created by or stored on a Department owned electronic communication system or device, i.e., cellphones, tablets, or IPads. The Department reserves the right to use the data and/or content for any purpose.

IV. TABLE OF ANNEXES

This directive has been arranged in Annexes to provide an easy reference.

ANNEX A Department Owned Computer Equipment

ANNEX B Email Usage

ANNEX C Internet Usage

Richard C. Smith
Chief of Police

Adopted by the Board of Police Commissioners this 31st day of August, 2021.

Mark C. Tolbert
Board President

DISTRIBUTION: All Department Personnel
Public View Master Index - Internet
Department Master Index – Intranet
Policy Acknowledgement SyStem (PASS)

ANNEX A

DEPARTMENT OWNED COMPUTER EQUIPMENT

A. The use of software/hardware on Department computers will be limited to lawful and productive endeavors.

B. The handling of any computer software will be as follows:

1. The unauthorized copying of Department computer software is prohibited.

2. Copies of the registration and/or license agreement will be forwarded and maintained in ISD.

3. All software must be reviewed by the ISD prior to being installed on any Department computer.

*C. Only ISD personnel, or an approved designee, will move, install or disassemble Department computer equipment, telephones, printers, and monitors. This includes all mobile devices and any peripheral computer equipment utilized at a Department facility or in a Department vehicle.

1. In an emergency situation in which a Department facility or vehicle is in danger of being compromised or destroyed, members may take action by removing the Department computer asset in order to preserve it.

2. The Technology Support Help Desk will be notified as soon as possible following an emergency event to initiate the actions to recover and secure the Department computer asset.

3. Mobile equipment (i.e. laptop, tablet, cellular phone) assigned to a member may be moved as required by their assigned duties.

*D. For the purposes of complying with Criminal Justice Information Services (CJIS) Policy Section 5.5.6.1, and electing to adopt a more strict state policy in this area, MULES prohibits BYOD from accessing, processing, storing or transmitting Criminal Justice Information (CJI). The Department's network, including e-mail, is considered a CJI network.

E. Non-Department personnel access to the Department network or computer applications.

1. When non-Department personnel (e.g. members of a task force, special assignment or internships) need access to the Department network, the element overseeing this individual (responsible element) will forward the

individual's information through the chain of command to the Administration Bureau Office for approval. The information will include what computer applications need to be accessed and a copy of the applicable Memorandum of Understanding, if one exists.

*2. When non-Department personnel no longer need access to the Department network, the responsible element will notify ISD through the Help Desk, so that access can be disconnected.

*F. Damaged or inoperable computer equipment will be reported in accordance with the guidelines set forth in the written directive entitled, "Department Property."

*G. Introducing Non-Department Programs, Developments, Applications, Software or other platforms to Department owned computer equipment.

1. All members who wish to introduce, implement, and/or use computer programs, developments, applications, software, or other platforms for Department related business, which are not presently being used, will:

a. Submit a written request via an Interdepartment Communication, Form 191 P.D., or Memorandum, through their chain of command to the Administration Bureau Commander for the review by the Information Technology Advisory Committee (ITAC).

b. A submission request will contain the following information:

(1) Program name and function.

(2) Company's or owner of the software name, address, and phone number of developer or owner of property rights.

(3) Brief synopsis of the program and intended uses including software/hardware, fees, costs, and ongoing operating costs.

2. ITAC will:

a. Review all Department member and/or unit submissions to create, develop or implement software, programs, applications, or other platforms to be used within the Department.

b. Ensure there are no programs that interfere or overlap in functions with other programs that are not a necessity for departmental operations.

c. Submit recommendations for approval to the Administration Bureau Commander, or designee.

d. Notify the member regarding any unapproved submissions.

e. Follow through with proper implementation and documentation of Department approved program, upon approval from the Executive Committee.

3. The Administration Bureau Commander, or designee, will:

a. Review and forward all ITAC recommended and/or approved requests to the Executive Committee for final approval.

b. Follow up with the ITAC regarding any recommendations that are unapproved.

ANNEX B

ELECTRONIC MAIL (E-Mail) COMMUNICATIONS

*A. Use of the e-mail system by any member implies both understanding and compliance with this directive and CJIS Security Policy (http://10.105.1.50/MULES/cjismanuals). Members using e-mail will do so in an appropriate and professional manner. E-mail that is distasteful, disruptive, offensive and unlawful will tarnish the professional image of the Department.

*B. All messages generated on or handled by Microsoft Outlook, including back-up copies, are considered property of the Department, not the member, and are subject to Sunshine Law requests with the exception of those covered by Attorney/Client Privilege or other confidentiality privileges, and is considered part of casefiles and subject to discovery.

C. Members will have no expectation of privacy in anything they store, send or receive on the e-mail system. The Department may monitor e-mail without prior notice to the member.

*D. E-mail is for official use only. If approved by the Chief of Police or designee, incidental personal use is permissible as long as it does not interfere with productivity or preempt official use or violate the written directive entitled, “Code of Ethics and Rules of Conduct.”

*E. Every Department member is required to use e-mail when on-duty and clean out their e-mail inbox on a regular basis to ensure timely dissemination of information. E-mail notifications are sent to Department members directing them to log into Policy Acknowledgement SyStem to review and electronically sign all newly issued directive(s).

ANNEX C

INTERNET USAGE

A. Members must use the Internet in accordance with all applicable laws and regulations. This includes compliance with copyright and license laws governing programs, as well as data and written materials accessed, obtained or provided to others via the Internet.

B. Members will not download software from the Internet without prior approval from Information Services Division.

NOTE: To prevent inadvertent downloading, Internet users should be wary of pop-up menus or advertisements that suggest doing so.

C. Prohibited uses of the Internet include but are not limited to the following:

*1. Using Internet connections for streaming services or private gain that violates the written directive entitled, “Code of Ethics and Rules of Conduct,” i.e., announcing garage sales or selling products for profit, or to solicit for political, religious, or other non-business purposes.

2. Deliberate attempts to degrade or disrupt system performance may be considered criminal activity with possible prosecution under applicable state and federal laws.

*D. The following websites and site categories will be blocked unless access has been authorized by the Helpdesk. Any element or individual requesting access must establish a business case and receive approval through their chain of command. Once approved, forward the request to the Helpdesk.

1. Gaming Sites – Any website that facilitates or promotes gambling

2. Pornographic and Adult Content Sites

3. Hate Sites – Any site sponsored by militant or extremist groups that promote racism and hateful opposition to or action against segments of the population.

4. Software Download and Installation – Downloading and installation of software from the Internet is a violation of current written directives.

*5. Uncategorized Uniform Resource Locators (URL) – URLs that are uncategorized many times contain malware; therefore, URLs lacking a category will need to be submitted to the Help Desk for approval to open.

E. The use of the Internet is not a private matter and the Department reserves the right to monitor all uses without notification to the member; audits will be conducted by the ISD, as required.