Information Technology Use

1503.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of office information technology resources, including computers, electronic devices, hardware, software and systems.

1503.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented or licensed by the Montgomery County Sheriff's Office that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Office or office funding.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, pagers, modems or any other tangible computer device generally understood to comprise hardware.

Software - Includes, but is not limited to, all computer programs, systems and applications including "shareware." This does not include files created by the individual user.

Temporary file, permanent file or file - Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs, audio or videos.

1503.2 POLICY

It is the policy of the Montgomery County Sheriff's Office that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Office in a professional manner and in accordance with this policy.

1503.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts or anything published, stored, shared, transmitted or maintained through file-sharing software or any Internet site that is accessed, transmitted, received or reviewed on any office computer or other system.

The Office reserves the right to access, audit and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received or reviewed over any technology that is issued or maintained by the Office, including the office email system, computer network, and/or any information placed into storage on any office system or device. This includes records of all key strokes or web-browsing history made at any office computer or over any office network. The fact that access to a database, service or website requires a user name or password or is the deputy’s personal email, Facebook or other person’s software will not create an expectation of privacy if it is accessed through office computers, electronic devices or networks.

1503.4 RESTRICTED USE

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to their supervisors.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

1503.4.1 SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes, in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any office computer. Members shall not install personal copies of any software on any office computer or modify any software or hardware.

When related to criminal investigations, software program files may be downloaded only with the approval of the information systems technology (IT) staff and with the authorization of the Sheriff or the authorized designee.

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Office while on office premises, computer systems or electronic devices. Such unauthorized use of software exposes the Office and involved members to severe civil and criminal penalties.

Introduction of software by members should only occur as a part of the automated maintenance or update process of office- or county-approved or installed programs by the original manufacturer, producer or developer of the software. Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

1503.4.2 HARDWARE AND DATA

Access to technology resources provided by or through the Office shall be strictly limited to office-related activities. Data stored on or available through office computer systems shall only be accessed by authorized members who are engaged in an active investigation, assisting in an active investigation, or who otherwise have a legitimate law enforcement or office-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

1503.4.3 INTERNET USE

Internet access provided by or through the Office shall be strictly limited to office-related activities. Internet sites containing information that is not appropriate or applicable to office use and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, gambling, chat rooms, and similar or related Internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member's assignment.

Downloaded information from the Internet shall be limited to messages, mail and data files.

1503.4.4 ON-DUTY USE

Members shall only use technology resources provided by the Office while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor. This prohibition includes the use of telephones, cell phones, texting, email or any other “off-the-clock” work-related activities. This prohibition also applies to personally owned computers that are used to access office resources. Personal communication devices, or PCD's, will not be used to access State, federal or office related programs, websites or documents.

Refer to the Personal Communication Devices Policy for guidelines regarding off-duty use of personally owned technology.

1503.5 PROTECTION OF SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from theft, physical and environmental damage and are responsible for the correct use, operation, care and maintenance of the computer system.

Members shall ensure office computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, logon information and other individual security data, protocols and procedures are confidential information and are not to be shared. Password length, format, structure and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor.

In regards to CJIS protocol, the computer mounted systems are to be password protected and safely locked and secured in each patrol car. The docking station that each individual car contains will have a key type lock which are to be kept locked at all times, with the key secured elsewhere.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any theft or unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a supervisor.

At the end of your shift it required that each user shall close out of all programs and properly shut down the computer to protect its inner workings, but also to protect the integrity of the material that it contains.

1503.6 INSPECTION AND REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, damage, computer system malfunctions, problems or general computer system failure, a lawsuit against the Office involving

one of its members or a member's duties, an alleged or suspected violation of any office policy, request for disclosure of data, or a need to perform or provide a service or pursuant to random inspections.

The IT staff may extract, download, or otherwise obtain any and all temporary or permanent files residing or located in or on the office computer system when requested by a supervisor or during the course of regular duties that require such information.