Information Technology Use

321.1 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.

321.1.1 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 St. Mary's 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.

Network - A global term that includes but is not limited to the definitions of "Hardware", "IT", "Software", "Files" and "Electronic Hand Held Devices" as set forth in this policy.

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 or videos.

321.2 POLICY

It is the policy of the St. Mary's 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.

321.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts or anything published, shared, transmitted or maintained through file-sharing software or any Internet site that is accessed, transmitted, received, or reviewed on any office computer 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 e-mail system, computer network or any information placed into storage on any office system or device. This includes records of all keystrokes 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 username

or password will not create an expectation of privacy if it is accessed through office computers, electronic devices or networks.

Although the Office may not require access to a member's personal accounts, it may require a member to disclose a username, password, or other means for accessing non-personal accounts or services that provide access to office computer or information systems (Md. Code LE § 3-712(b)).

321.4 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 or Shift 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.

321.4.1 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.

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.

IT personnel will do all software installation or MDB repair or an IT approved contractor.

IT will install and/or ensure antivirus updates are current.

321.4.2 HARDWARE

Access to technological 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.

321.4.3 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. Files authorized for download from the Internet must be scanned with virus detection software before being opened.

Alternate Internet Service Provider connections to St. Mary's County Government's internal network are not permitted unless expressly authorized by the St. Mary's County Government Information Technology Department and properly protected by a firewall or other appropriate security device(s) and/or software.

321.4.4 OFF-DUTY USE

St. Mary's County information systems are provided for and must be used only for business purposes. Incidental personal use is permissible if the use:

(a) Does not consume more than a trivial number of resources that could otherwise be used for business purposes.

(b) Does not interfere with worker productivity.

(c) Does not preempt any business activity; Is not illegal or unethical.

(d) Permissible incidental use of an electronic mail system would, for example, involve sending a message to schedule a luncheon.

Members shall not use St. Mary's County information systems for operating a business, soliciting money for personal gain, or otherwise engaging in commercial activity outside the scope of employment.

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

321.5 PROTECTION OF SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from 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 protection 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.

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 unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a supervisor.

If any problems occur with the telephone system, computers, or any other electronic equipment, the St. Mary's County Information Technology Department (IT) will be notified for assistance.

Members may not make changes, additions, or deletions to the core system software or standard desktop configuration. If members need additional hardware or software to perform his/her job, such as a project-specific application program, the member should notify the IT Department via their supervisor of this requirement.

321.6 COMPUTER ADMINISTRATION

Key Cards for the Sheriff's Office Headquarters and Circuit Courthouse will be created and managed by the systems administrator using the WinDSX program. Key card access will be programed as directed by the Administrative Division Commander and Judicial Unit supervisor respectively.

321.7 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, 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.

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.