Information Technology Use

321.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of agency 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 Milwaukee County 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 County or county funding.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, 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, or videos.

321.2 POLICY

It is the policy of the Milwaukee County Sheriff's Office that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the County 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 county computer system.

The County 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 County, including the county email system, computer network, and/or any information placed into storage on any county system or device. This includes records of all keystrokes or Web-browsing history made at any county computer or over any county 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 county computers, electronic devices, or networks.

The County will not request or require, as a condition of employment, that employees disclose access information for their personal Internet accounts or otherwise grant access to, or allow observation of, those accounts unless specifically permitted to do so under federal or Wisconsin law (Wis. Stat. § 995.55).

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 Commanders.

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 county computer. Members shall not install personal copies of any software onto any county computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the Information Management Services Division (IMSD) and with the authorization of the Criminal Investigation Division supervisor or the authorized designee.

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

Introduction of software should only occur as part of the automated maintenance or update process of County-approved or installed programs by the original manufacturer, producer or developer of the software.

Any other introduction of software requires prior authorization from IMSD and a full scan for malicious attachments.

321.4.2 HARDWARE

Access to technology resources provided by or through the County shall be strictly limited to county-related activities.

321.4.3 INTERNET USE

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

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

321.4.4 OFF-DUTY USE

Members shall only use technology resources provided by the County while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor. This includes the use of telephones, cell phones, texting, email or any other “off the clock” work-related activities. This also applies to personally owned devices that are used to access county resources.

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

321.5 PROTECTION OF COUNTY 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 county 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 IMSD.

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.

321.6 INSPECTION OR REVIEW

Reasons for inspection or review of the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof may include, but are not limited to, routine supervisory inspection or inspection based on cause, computer system malfunctions, problems or general computer system failure, a lawsuit against the County involving one of its members or a member’s duties, an alleged or suspected violation of any agency or county policy, a request for disclosure of data, or a need to perform or provide a service.

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