Information Technology Use

321.1 PURPOSE AND SCOPE

Best Practice MODIFIED

The purpose of this policy is to provide guidelines for the proper use of Department of State Hospital (DSH) information technology resources, including computers, electronic devices, hardware, software and systems (see AL 2014-04-Email/PDF Policy, State Administrative Manual, Section 4500-Telecommunications, Policy Directive 7102-State Issued Mobile Device Policy and Gov. Code § 11152).

321.1.1 DEFINITIONS

Best Practice MODIFIED

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 California Department of State Hospitals 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 OPS or OPS 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 and firmware. 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

Best Practice MODIFIED

It is the policy of DSH that employees shall use information technology resources, including computers, software and systems, that are issued or maintained by DSH in a professional manner and in accordance with this policy.

321.3 PRIVACY EXPECTATION

State MODIFIED

Employees 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 department computer system.

DSH 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 DSH, including DSH email system, computer network

and/or any information placed into storage on any DSH system or device. This includes records of all keystrokes or Web-browsing history made at any DSH computer or over any DSH 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 DSH computers, electronic devices or networks.

However, DSH may not require an employee to disclose a personal username or password or pen a personal social website, except when access is reasonably believed to be relevant to the investigation of allegations of work-related misconduct (Lab. Code § 980).

321.4 RESTRICTED USE

Best Practice **MODIFIED**

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

Employees 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

Best Practice **MODIFIED**

Employees 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, employees shall not install any unlicensed or unauthorized software on any DSH computer. Members shall not install personal copies of any software onto any DSH 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 Chief of Law Enforcement or the authorized designee.

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

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

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

321.4.2 HARDWARE

Best Practice **MODIFIED**

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

321.4.3 INTERNET USE

Best Practice **MODIFIED**

Internet access provided by or through the OPS shall be strictly limited to OPS-related activities. Internet sites containing information that is not appropriate or applicable to DSH 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.

321.4.4 OFF-DUTY USE

Best Practice **MODIFIED**

Employees shall only use technology resources provided by DSH 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 DSH resources.

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

321.5 PROTECTION OF SYSTEMS AND FILES

Best Practice **MODIFIED**

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 DSH 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 TSD staff or a supervisor. Passwords for accounts that access CJI are governed by the CJIS Access, Maintenance, and Security Policy.

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

Best Practice **MODIFIED**

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 DSH involving one of its employees or an employee's duties, an alleged or suspected violation of any DSH policy, a request for disclosure of data, or a need to perform or provide a service.

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