Information Technology Use

321.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of department 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 Brea Police Department 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 Department or department 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 or videos.

321.2 POLICY

It is the policy of the Brea Police Department that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Department 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 department computer system.

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

The Department shall not require a member to disclose a personal username or password for accessing personal social media or to open a personal social website; however, the Department may request access when it is reasonably believed to be relevant to the investigation of allegations of work-related misconduct (Labor Code § 980).

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 Watch 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 department computer. Members shall not install personal copies of any software onto any department 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 Police or the authorized designee.

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

Introduction of software by members should only occur as part of the automated maintenance or update process of department- or City-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.

321.4.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to department-related activities. Data stored on or available through department computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or department-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 Department shall be strictly limited to department-related activities. Internet sites containing information that is not appropriate or applicable to department 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 shall be limited to messages, mail, and data files.

321.4.4 OFF-DUTY USE

Members shall only use technology resources provided by the Department 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 department resources.

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

321.5 PROTECTION OF AGENCY 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 department 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.

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

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 Department

involving one of its members or a member's duties, an alleged or suspected violation of any department policy, a 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 department computer system when requested by a supervisor or during the course of regular duties that require such information.

321.7 SANITATION AND DESTRUCTION OF ELECTRONIC AND PHYSICAL MEDIA

Per FBI Criminal Justice Information Services (CJIS) security policy sections 5.8.3 and 5.8.4, destruction of department electronic and physical media shall be carried out by authorized City Department Staff. The authorized employee(s) shall sanitize, that is, overwrite at least three times or degauss, digital media prior to disposal or release for reuse by unauthorized individuals.

Inoperable digital media is destroyed by physical breaking the platens of the hard drive disks. Authorized Information Technology employees shall ensure the sanitization or destruction is logged, witnessed and carried out by authorized personnel. All paperwork is shredded by an escorted shredding service and witnessed by police department employees.

321.8 MANAGING SYSTEM ACCOUNTS

Per FBI Criminal Justice Information Services (CJIS) security policy section 5.5.1, authorized City Department Staff (System Administrators) shall manage police department employees' information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. They shall validate information system accounts at least annually and shall document the validation process. Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. They shall identify authorized users of the information system and specify access rights/privileges. They shall grant access to the information system based on valid need-to-know/need-to-share that is determined by assigned official duties; and satisfaction of all personnel security criteria. The authorized employees responsible for account creation shall be notified by an authorized police department employee when a user's information system usage or need-to-know or need-to-share changes and when a user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

321.9 CJIS COMPLIANCE

In accordance with CJIS policies:

- All patches for applications such as CAD I RMS, including public safety mobile applications, are thoroughly vetted and tested by the appropriate vendor and then by Brea IT staff members prior to the installation of them.
- Prior to installation of patches and hotfixes, backups are performed in the event the organization needs to undo/ rollback the changes that were made.
- Brea PD does not perform unattended I automatic updates. Updates and patched to PC's and systems are planned and scheduled.

- Brea uses centralized software management to push out Microsoft security updates.

All updates / hot fixes I patches are continuously monitored by our technical staff and support vendors.

321.10 SANCTIONS FOR MISUSE

Each suspected incident of unauthorized or improper use of CLETS equipment or criminal justice information or failure to take physical security measures to protect CLETS equipment or criminal justice information will be investigated. Violations will result in disciplinary actions which may include the employee's loss of use or limitations on use of equipment, discipline up to and including termination, criminal penalties, and/or financial liability for the cost of improper use.