Information Technology Use

324.1 IT 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.

324.1.1 IT 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 Unified 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, 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.

324.2 IT POLICY

It is the policy of the UPD 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.

324.3 IT PRIVACY EXPECTATION

Members forfeit any expectation of privacy regarding emails, texts, or anything published, shared, transmitted, or maintained through file-sharing software or any Internet site that is accessed, transmitted, received, stored, or reviewed on any department-issued hardware.

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 provided, funded, 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 may not require a member to disclose a username and / or password that allows access to the member's personal Internet accounts, except as may be provided in UCA 34-48-201.

324.4 IT 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 supervisor(s) or shift sergeant(s).

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.

324.4.1 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 or maintain any personal copies of any software on any department computer.

When related to criminal investigations, software program files may be downloaded by those properly trained to recover such evidence and only with the approval of the information systems technology (IT) staff and with the authorization of the Chief 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, 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 the Technical Services Commander, and a full scan for malicious attachments.

All software installed onto any department computer after the initial authorized imaging must be approved by the member's Commander / Administrator and the Technical Services Commander.

Computer software must be loaded:

a. as received from the manufacturer, or
b. installed from the UPD or County network server, or
c. scanned and cleaned with approved anti-virus software prior to installation, and
d. installed by an authorized Technical Services or County computer technician with administrative rights.

(For assistance on desk-top systems contact the County Information Services. For assistance on lap-top systems contact the Technical Services technician.)

324.4.2 TRACKING AND CONTROL OF SOFTWARE LICENSES

1. All software purchased in bulk will be designated as a controlled asset within the inventory system. This will generally include operating systems and other programs loaded into every computer.

2. Special-use software, purchased at the Precinct / Division level for specific applications, will be documented on a controlled asset form by the respective Commander / Administrator. The form and copies of the software license documentation will be submitted to the department assets for review and classification. The form will include a description of the software type, a brand name, version, purchase date, and computer upon which it is installed. Original documentation will be retained by the Precinct / Division where the software is being used.

324.4.3 HARDWARE

Unless otherwise authorized, access to technology resources provided by or through the department shall be 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 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 and the involved member's Commander / Administrator.

324.4.4 INTERNET USE

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 and the member's Commander /

Administrator as a function of a member's assignment.

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

Also refer to the UPD Social Media Policy.

324.4.5 OFF-DUTY USE

Members participating in secondary off-duty employment may use the resources of the department within the same constraints as their on-duty usage, or as directed by policy.

Members are held to the same standards for using their information technology resources off-duty that they are while on-duty. "Curiosity checks," as understood by BCI, are not permitted.

The viewing of digital video and / or audio recordings by members engaged in secondary off-duty employment shall be limited to those recordings that would not shock the general public.

At no time may members view any recording on department technology rated over MPAA R-Restricted while engaged in secondary off-duty employment or on-duty employment regardless of the resource used to view the recording.

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

324.4.6 AGENCY PROPERTY

All information, data, documents, communications, and other entries initiated on, sent to or from, or accessed on any department computer, or through the department computer system on any other computer, whether downloaded or transferred from the original department computer, shall remain the exclusive property of the department and shall not be available for personal or non-departmental use without the expressed authorization of a member's Commander / Administrator.

324.4.7 ACCEPTABLE USE OF DEPARTMENT INFORMATION TECHNOLOGY

1. Members may not allow unauthorized individuals access to department IT resources without written permission from the Chief.

2. Department resources will not be used to harass any other person or expose the UPD to libel. Harassment covers any use of department resources to contact any person directly or indirectly in an unwanted fashion. Harassment can be active, in forms such as unwanted e-mail, chat messages, or verbal declarations on a public forum, or can be passive in the form of defamatory information posted on websites.

3. No member will access questionable websites or content unless the access is within the scope of their assignment. Under no circumstances will members access pornographic content either on the Internet, through a removable media (CD-RO, USB drive, etc.), or via any computer or device they have access to without receiving approval from their supervisor and Commander / Administrator and by obtaining a case number and generating a General Offense report.

4. Members will not use services such as Internet or Peer-to-Peer file sharing, music and / or recording sharing or photo sharing software without the written approval of permission of the Commander / Administrator.

5. Other references may include portions of this Manual, but not limited to: Electronic Mail Policy, Personal Communication Devices Policy, and Employee Speech, Expression, and Social Networking Policy.

324.5 PROTECTION OF UNIFIED POLICE DEPARTMENT OWNED COMPUTER SYSTEMS

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 Technical Services, County 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.

Documents, spreadsheets, or other information exchanged on removable computer media (e.g. discs, CDs, USB devices, etc.) are the most common method of spreading computer virus. Any media introduced into Unified Police Department / Salt Lake County systems must be approved through the chain of command; including the Technical Services Commander and County IT prior to installation.

Any discovery of a computer virus should be immediately reported to the County Information Systems Help Desk.

All product copyright and license requirements will be strictly adhered to.

Physical modification or damage to computer equipment is prohibited.

Beverages or food items will not be placed or held in a position that would allow for accidental spills to occur onto computer equipment.

Changes to the configuration of a computer system, such as the addition of memory, drive space, updated sound, or video components, must be approved through the chain of command to the members Commander / Administrator.

The hard drive of a personal computer, laptop, or mobile data computer that is designated as surplus will be removed and destroyed by the UPD Assets Supply Coordinator. The hard drive of a personal computer, laptop, or mobile data computer that is transferred to another user will be cleaned and reimaged by a Technical Services or County technician, as applicable.

324.5.1 INFORMATION TECHNOLOGY SYSTEM ACCESS PROCEDURE

1. A member requiring access to any UPD Information System will request access through their supervisor. The supervisor will send a request to their Commander / Administrator recommending level of access and resources requiring access to including e-mail, RMS, MDC MRE, CAD, File Server, UCJIS, ULEIN, or any other pertinent systems, websites, or accounts.

2. Changes in access level through transfer, promotion, termination, or changes in access requirements will require a request from the member's supervisor to their Commander / Administrator.

3. The Commander / Administrator will forward the request to Technical Services Commander for review and action. The Commander / Administrator will specify approval for the requested systems, websites, or accounts. Systems that require licensing and accompanied by a corresponding cost must be approved by the Commander / Administrator.

324.5.2 IT SECURITY AND ACCESS PROCEDURE FOR EXTERNAL AGENCY USERS

External agencies and / or member(s) thereof requesting access to the UPD information or data systems must submit a written request, from their agency head to the Chief. The Chief or authorized designee, upon approval of the request, will forward it to the Technical Services Commander / Administrator for implementation. Those agencies covered by interlocal agreement(s) through association with an approved UPD member task force function shall be deemed to have received such pre-approval.

324.6 IT INSPECTION OR REVIEW

1. 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.

2. 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.

3. The IT staff or Technical Services technician may extract, download, or otherwise obtain all temporary or permanent files residing or located in or on the department computer system when requested by a supervisor and through the written approval of the member's Commander / Administrator, by the Internal Affairs Unit, or during the course of regular duties that require such information.

4. Any software, files, correspondence, or other information found on the system or device that does not correspond to department policy will be documented and removed by IT Staff or a Technician from Technical Services. Documentation of the offending items will be forwarded to the Technical Services Commander who shall notify the Commander / Administrator of the involved officers' system for appropriate action.

324.7 COMPLIANCE WITH I.S. POLICIES REQUIRED

1. This policy requires all requests for computing or networking services, equipment and software shall be coordinated and reviewed with Information Services (IS).

2. All decisions as to computing or networking services, equipment, and software shall be made in accordance with the Computing Standards and Networking Standards established by IS.

3. If IS does not concur with department's networking request and the department desires to proceed, the request shall be brought before the Chief for final resolution.

324.7.1 STANDARDS OF CONDUCT

It is a violation of the standards of conduct to use e-mail or the internet to harass or discriminate based on sex, race, religion, color, national origin, age, disability, sexual orientation, or marital status.

324.7.2 E-MAIL, VOICE MAIL AND INTERNET ACCEPTABLE USE POLICY

1. All e-mail correspondence using UPD / County systems and equipment is the property of UPD.

2. Limited personal use of e-mail is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in disciplinary action. Personal e-mail shall not impede the conduct of department business.

3. Limited personal use of the internet is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in disciplinary action

as provided in UPD Member Misconduct and Discipline Policies. Personal use is permissible so long as it: (a) does not interfere with worker productivity and (b) does not preempt any business activity.

4. Personal use of the internet during authorized breaks should be limited as much as practicable to areas out of sight and sound of the public and shall not be disruptive to the work environment.

5. The use of department resources, including electronic communications, should never create the appearance of inappropriate use.

6. Internet connection is only allowed through UPD / Salt Lake County Information Services unless explicit approval of the Chief is obtained.

7. Additional requirements and restrictions are detailed in each specific policy.

324.7.3 INTERNET / INTRANET ACCESS LEVELS

Definitions:

Level One Access is open access to UPD Internet, Intranet, and standard e- mail.

Level Two Access is filtered access to UPD Internet, Intranet, and standard e-mail.

Level Three Access is UPD Intranet and e-mail.

Access Level Guidelines:

a. All requests for Internet / Intranet access must be approved by the Commander / Administrator. The Commander / Administrator will be responsible for ensuring all levels of access are being used properly and for official UPD business.

b. An access list will be reviewed annually to determine if approved members still require the level of access currently held.

c. Commanders / Administrators will submit approved requests to the Chief. Information Services will only implement requests that are forwarded by the Chief.