8400 INFORMATION TECHNOLOGY

8410 GENERAL

The department's Information Technology (IT) support is provided by the City of Tucson's Information Technology (IT) Department, which provides electronic data processing and Internet and Intranet systems to members and to the public.

The City of Tucson's information systems are to be used in conjunction with the performance of a member's authorized duties and in accordance with Administrative Directives (AD)1.08-3 (Information Security) and 1.08-4 (E-mail). While using the city's information systems, members shall conduct themselves in a professional manner.

8411 **Policies**

The city provides electronic and telephonic communications, including e-mail, Internet/Intranet access, voice mail, and other systems ("city electronic communication systems") to its employees and other authorized individuals "(authorized users") for their use in performing city duties or business.

City electronic communication systems are to be used for city business, except as specifically allowed by this policy. In addition to any other civil or criminal sanctions available to the city under law, any authorized user who uses a city electronic communication system in a manner inconsistent with this policy or in violation of any other city policy is subject to the following:

- If an employee, disciplinary action up to and including termination.
- If a non-employee, immediate loss of the privilege to use any city electronic communication system, and contract revocation.

City electronic communication systems, and the electronic communications or information transmitted or stored on these systems, are the sole property of the city, and authorized users have no personal or property rights in them.

This policy applies to all city electronic communication systems, including but not limited to telephones, mobile phones, wireless communication devices, PDA devices, the City's data network, and personal computers; and all who access these systems. The term computer includes any laptop, desktop, or tablet.

Authorized users may use city electronic communication systems for performing city business. City electronic communication systems are provided by the city solely for authorized users' (business use during city time), and shall be used in a professional and courteous manner. Authorized users shall use the same professional courtesy in electronic communications as in other verbal written communications. All department computers are subject to random audit at the discretion of the City IT Public Safety Administrator. Audit of passwords, access codes and access violations shall occur semi-annually. The semi-annual audit will be completed by the System Security Officer – Terminal Agency Coordinator during the TOC audit. The City of Tucson IT Department will review audit logs for any alerts. The Arizona Department of Public

Safety ISO and Access Integrity Unit will be notified, by the TAC/SSO immediately of any breaches in system security.

Incidental use of City electronic communication systems (sending or receiving) for personal, non-business purposes is permitted under the following conditions:

- Personal use is limited to non-work hours (before/after work, breaks or lunch time in accordance with building access hours);
- Personal use may not interfere with the productivity of the authorized user or his or her co-workers;
- Personal use may not be performed in areas where there is direct interaction or service to the public;
- Personal use may not involve any prohibited activity described in this policy;
- Personal use may not disrupt or delay the performance of City business;
- Personal use may not consume city resources or otherwise deplete system resources available for business purposes.

If the personal use of city electronic communication systems results in a cost to the city, the authorized user must reimburse the city.

Any use of city electronic communication systems that violates any law, regulation, ordinance, policy or procedure of the city is forbidden.

As stated in *City Policy 1.08-3* "Information System Security," authorized users may not load any software on city computers, including freeware and shareware available from internet sites.

City electronic communications systems shall not be used in any way that is offensive, harmful, or insulting to any person. Examples of forbidden electronic communications include, but are not limited to:

- Threatening, harassing, obscene or of a profane nature, or that which would be considered to be offensive or disruptive or to infringe on the personal privacy of others;
- Gambling;
- Ethnic or racial slurs;
- Unsolicited "junk mail", "for profit" messages, or chain letters;
- Sexually explicit photography, messages, jokes/cartoons;
- Unwelcome propositions, or any other use that violates the City's nondiscrimination and harassment policies;

- Signed or identifies as coming from an individual other than the actual sender, unless the sender is authorized to send that type of electronic communication on behalf of the other individual (e.g. a secretary's e-mail meeting notice in a supervisor's name, when authorized by the supervisor);

- In support of or connection with the authorized user's own outside employment or business activity (e.g. commercial consulting for pay, solicitation or sales of goods or services, administration of the business or employment).

Authorized users who are unsure whether an electronic communication is authorized should check with a supervisor prior to sending it.

If an electronic communication is received that is thought to contain prohibited content, the receiver shall report the matter to a supervisor for appropriate action.

City electronic communication systems shall not be used to copy, send or receive copyrighted materials, trade secrets, proprietary financial information, or similar materials without appropriate authorization.

City electronic communication systems shall not be used to transmit political messages.

Authorized users are prohibited from undertaking any unauthorized access, reading, modifying, copying, transferring, or deleting any other authorized user's electronic communications or information, computer or network equipment, or security controls.

Any attempt to bypass city computer/network security controls is forbidden. E-mail shall not be used to maintain or store official city records or other information.

Authorized users shall not register their city e-mail address at Internet sites unless necessary to conduct city business.

The Chief of Police or designee shall approve department-wide e-mails. Citywide e-mails shall be approved by the City Manager's office.

All city hardware, software, temporary and permanent files, and related systems or devices that are used to access, transmit, receive, or store electronic communications or information, and the electronic communications and information themselves, are city property.

The city has the right to access electronic communications or information transmitted by or stored on city electronic communication systems at any time, with or without prior notice to authorized users. Authorized users have no expectation of privacy with respect to any use, professional or personal, of city electronic communications systems.

The City reserves the right to delete any electronic communication or information received through any city electronic communication system in order to maintain effective and efficient operation of the city's systems. Electronic communications may be deleted at any time, with or without prior notification.

Additionally, electronic communications may be subject to a public record request under the Arizona Public Records Act, and therefore subject to public disclosure. Authorized users shall exercise the same level of care in using electronic communications that they would exercise for composing and sending communications set down on paper. This statement of policy is not a statement or admission by the city that any particular electronic communication is in fact subject to disclosure under the Arizona public Records Act. That determination will be made on a case-by-case basis.

Authorized users should avoid using city electronic communication systems to send confidential, privileged, and/or sensitive information. Authorized users must exercise caution in transmitting confidential information by e-mail and/or the Internet/Intranet, because of the ease of redistributing such information. Confidential information must never be transmitted to anyone who is not authorized to receive such information.

The IT Department (or its authorized agents) is responsible for managing electronic communication systems, and establishing the appropriate standards and procedures to ensure the security and availability of the system. This includes procedures for routinely purging stored electronic communications. The City IT Department is responsible for maintaining the City Network and the TPD Network.

8420 HARDWARE

All requisitions to purchase computers or equipment for Department owned computers must be approved by the City IT Public Safety Administrator. The installation of the computer or equipment will be accomplished and recorded by the City IT support staff unless the City IT Public Safety Administrator has granted prior approval for the installation.

The Support Services Bureau Commander or the City IT Public Safety Administrator shall determine the priorities that will be used in governing department allocation of computer systems and or peripheral hardware.

Employees shall notify the City IT Public Safety Administrator of any changes in computer configurations and/or relocations of any computer equipment in order to maintain accuracy of the inventory. If a computer is being transferred to another unit, the units involved must fill out proper paperwork.

8430 SOFTWARE

8431 General

Members shall not perform any unauthorized duplication or distribution of copyrighted software on city equipment. Additionally members shall not duplicate or distribute software licensed to the City of Tucson for private use or for sale to third parties. Computer software not purchased by the department shall not be used on department computers unless authorized by the City IT Public Safety Administrator. A *Software Justification* form is available on the TPD shared drive that shall be filled out and sent to the City IT Public Safety Administrator for action.

If the software is approved, the City IT Public Safety Administrator will start the requisition process. The installation of this software will be accomplished and recorded by the City IT support staff unless prior approval for the installation has been granted. City IT will retain and store the software media and license documentation.

Computer software is to remain on the machine for which it was intended, unless the removal from one machine and installation on another machine is authorized by the commander(s) of the affected unit(s) and by the City IT Public Safety Administrator. Copies of this software shall not be installed on other Department machines or any privately owned machines unless the license allows for this and the City IT Public Safety Administrator has authorized it.

8432 Electronic Information Transfers

City IT support staff will be the only employees to download software unless prior approval has been granted by the City IT Public Safety Administrator.

8433 Documentation

The Division Commander or administrator of units developing, modifying, or using software programs for specific applications shall be responsible for ensuring that proper documentation is done in a timely manner. This documentation may include:

- A written narrative describing the programs, files, and procedures used by the system
- System or program requests and appropriate responses
- Program source code listings
- Records formats showing sequence of data elements and character length of all files accessed
- Samples of source documents, displays, and reports
- Description of backup procedures and frequency
- List of authorized operators
- Any special requirements an individual system may require

A current and complete copy of the above documentation shall be provided to the Data Services Section for filing.

8434 Manuals

Documentation for software shall stay at the location of the machine on which the software is installed, unless the commander or administrator of the unit, section, etc. specifically authorizes the loaning of the documentation

8440 BACKUP FILES

8441 Individual Users

Although usually reliable, computers sometimes fail and the users of computers must practice adequate backup procedures so that restoration of the work product can be achieved. These procedures are established to assist department employees in maintaining adequate backup

copies of data/user files. The City IT Support staff will back up files contained on the TPD servers on a regular basis.

If a user must maintain data information somewhere other than a TPD server (the local C and/or D drive), it is the responsibility of the user's Unit Supervisor to insure that an adequate backup system is established and maintained. The backup system will consist of two copies:

- A backup copy kept in a location facilitating timely updating
- A master backup copy kept in a secure location removed from the area of the local copy. Data Services has an area which can be used for this storage.

The frequency of updating the master copies, as well as the required degree of security for these copies, will vary depending upon the nature of the data. However, in all cases the master copy shall be updated at least once every month and secured away from the local backup copy. On a quarterly basis, Unit supervisors shall insure that proper backups are being done.

8442 Department Systems

Department systems contain security protocols that are verified periodically. Back-up systems are monitored and tested regularly.

8450 DEPARTMENT WEB SITES

8451 General

While Internet/Intranet technologies may be used with good intent in promoting communication among members, the establishment of independent web sites on non-city web servers that purport to be sanctioned by the Tucson Police Department is not permitted. All patches, badges, logos and emblems of the city of Tucson and the Tucson Police Department are copyrighted and shall not be reproduced on any web site without written permission from the Chief of Police.

8452 Guidelines

All department members shall adhere to the following guidelines when creating information for display on the Department's Internet web site.

- **Approval:** Information destined for publication on the department's web site shall follow approval procedures established by a division commander.
- **Format and style**: The department webmaster has the responsibility for placing information on the web site. Information may be submitted in various formats agreeable to the department webmaster.
- **Web page authoring:** If a unit wishes to place information on the web site, that unit assumes the responsibility for providing the content. An individual from that unit shall be assigned the responsibility to maintain the content and keep it current, accurate and easily understood by the public.

- **Statistical Information**: In order to ensure consistent statistical information throughout the entire web site, statistical information shall be created and maintained by procedures approved by a Bureau Commander or the Chief of Staff prior to publication.

- **Analysis and interpretation**: The Tucson Police Department does not characterize particular geographical locations of the city as “good” or “bad”. Crime and police incident information obtained via the web site and given to private parties shall be provided without comment. Members of the public can analyze the information themselves and arrive at their own conclusions.