Information Technology Appropriate Use Policy

209.1 PURPOSE AND SCOPE

The purpose of this policy is to ensure an information technology infrastructure that promotes the basic missions of the city. This policy aims to promote the following goals:

(a) To ensure the integrity, reliability, availability, and superior performance of it systems;

(b) To ensure that it systems are used for their intended purposes;

209.1.1 REASONS FOR POLICY

Information technology ("IT"), the vast and growing array of computing and electronic data communications facilities and services, is used daily to create, access, examine, store, and distribute material in multiple media and formats. Information Technology plays an integral part in the City's daily functions. Users of the City's IT resources have a responsibility not to abuse those resources. This City of Azusa IT Appropriate Use Policy (the "Policy" or "AUP") provides guidelines for the appropriate use of the City's IT resources as well as for the employees' access to information about and oversight of these resources.

Most IT use parallels familiar activity in other media and formats, making existing City policies important in determining what use is appropriate. Using electronic mail ("e-mail") instead of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor does it alter the guiding policies. City policies that already govern freedom of expression and related matters in the context of standard written expression govern electronic expression as well. This Policy addresses circumstances that are particular to the IT arena and is intended to augment but not to supersede other relevant City policies, resolutions, federal, state or local law.

For statements of other applicable City policies, resolutions, or local laws, consult the Personnel Manual, Records Retention Schedule as well the Municipal code.

209.1.2 DEFINITIONS

IT systems: these are the computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by the City of Azusa. For example, it systems include departmental and City-wide Information Systems, internet access, e-mail, desktop computers, laptop computers the network, PDA devices, phones, cell phones and other devices supported by it.

(a) **User**: A "User" is any person, whether authorized or not, who makes any use of any IT System from any location.

(b) **Systems Authority**: While city of Azusa is the legal owner or operator of all IT Systems, it delegates oversight of all systems to the IT Department, in the case of IT systems purchased with non-IT or other funds, this oversight is still provided by the IT Department.

(c) **Systems Administrator**: The IT Director may designate another person as "Systems Administrator" to manage the particular system assigned to a specific department. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT resources related to that system.

209.2 APPROPRIATE USE OF IT SYSTEMS

Although this policy sets forth the general parameters of appropriate use of it systems, departments may have policy manuals with detailed statements on permitted use and the extent of use that the city considers appropriate. In the event of conflict between policies, this appropriate use policy will prevail.

209.2.1 APPROPRIATE USE

IT Systems may be used only for their authorized purposes -- that is, to support the functions of the City of Azusa. City technology is made available for the purpose of increasing the effectiveness of communications, providing for increased productivity and facilitating research required to perform City related tasks. The particular purposes of any IT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the User.

209.2.2 PROPER AUTHORIZATION

Users are entitled to access only those elements of IT systems that are consistent with their authorization.

209.2.3 SPECIFIC PROSCRIPTIONS ON USE

The following categories of use are inappropriate and prohibited:

(a) Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading e-mail or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large e-mail messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

(b) Use that is inconsistent with City's Policy Procedures. The City is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-City purposes is generally prohibited, except if specifically authorized and permitted by the City Mangers Office.

(c) Use of IT Systems in a way that suggests City endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT Systems for the purpose of lobbying that connotes City involvement.

(d) Harassing or threatening use. This category includes, for example, display or access to offensive, sexual material in the workplace and repeated unwelcome contacts with another employees. The use of derogatory, obscene, suggestive, defamatory, or harassing language in the E-mail system or on the Internet.

(e) Use damaging the integrity of City IT Systems. This category includes, but is not limited to, the following six activities:

1. Attempts to defeat system security. Users must not defeat or attempt to defeat any IT System's security for example, by "cracking" or guessing and applying the identification or password of another User, or compromising room locks or alarm systems. (This provision does not prohibit, however, ITS or Systems Administrators from using security scan programs within the scope of their Systems Authority.)

2. Unauthorized access or use. The City recognizes the importance of preserving the confidentiality of Users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

3. Disguised use. Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized(i.e. guest user)

4. Distributing computer viruses. Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

5. Modification or removal of data or equipment. Without specific authorization, Users may not remove or modify any City-owned or administered equipment or data from IT Systems.

6. Use of unauthorized devices. Without specific authorization, Users must not physically or electrically attach any additional device (such as an external disk, printer, or video system) to IT Systems.

(f) Use in violation of law. Illegal use of IT Systems -- that is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited.

(g) Use in violation of City contracts. All use of IT Systems must be consistent with the City's contractual obligations, including limitations defined in software and other licensing agreements.

(h) Use in violation of City policy. Use in violation of other City policies also violates this AUP. Relevant City policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment.

209.2.4 PERSONAL ACCOUNT RESPONSIBILITY

Users are responsible for the security of their own it systems passwords. Any user changes of password must be requested through the IT department and done by IT staff. Accounts and passwords are normally assigned to single users and are not to be shared with any other person without authorization users are presumed to be responsible for any activity carried out under their it systems accounts.

209.2.5 RESPONSIBILITY FOR CONTENT

Official City information may be published in a variety of electronic forms. The Department under whose auspices the information is published is responsible for the content of the published document.

209.2.6 E-MAIL

When sending or receiving E-mail, the following considerations apply:

(a) Carefully select the recipients to receive an E-mail. Send only to those that need the information.

1. Transmitting the City's confidential information/data or sensitive information over unsecured E-mail is prohibited, unless expressly authorized by your departmental management.
2. Regularly check, open, read, and respond to E-mail sent to you. Response within 1 business day is recommended.
3. Delete old messages on a regular basis.
4. When using E-mail, extreme care must be exercised when downloading attachments. Attachments must be scanned for possible viruses.
5. Never open any unsolicited E-mail.
6. Questions regarding E-mail and the Internet should be addressed to the City Information Technology Help Desk.
7. E-mail responses sent to the public taking a position on an issue that may later need to be supported by management, or commenting on what would be considered a sensitive issue, should be at the direction of a Department Head or City Manager, with either the Department Head or City Manager being "copied" on the message.
8. Most communications (including E-mail) among City employees are not considered confidential. However, certain communications, personnel records

and police investigations, may be confidential and should be discussed with the employee's supervisor prior to use of E-mail.

9. Employees shall exercise caution in sending confidential information on the E-mail system as compared to written memoranda, letters or phone calls, because once sent, E-mail can not be retracted or controlled.

10. Confidential information should not be sent or forwarded to individuals or entities not authorized to receive that information and should not be sent or forwarded to other City employees not directly involved with the specific matter and expressly authorized to view.

11. Requests for employee access to the Network and E-mail systems should be made by the employee's division manager and sent to the Information Technology help desk.

12. Department heads must authorize requests to Technology Services for accounts for temporary or contract employees.

13. Departments requesting technology access for a temporary employee must inform Technology Services to remove E-mail access for that employee at termination.

14. The use of the City E-mail system for the advertising of personal items or services is unacceptable.

15. Reading someone else's E-mail without authorization is considered inappropriate. While no E-mail to a City E-mail address is considered private, confidential matters may be discussed over E-mail therefore proper business etiquette dictates that proper authorization be obtained before reading another person's E-mail.

16. Do not send E-mail under someone else's name.

(b) The City recognizes that there are times when electronic communications are appropriate which are not strictly speaking concerning City business. Such instances include death announcements, birth announcements, etc. Such uses of electronic communication are acceptable when done in accordance with all other aspects of this policy. When doubts arise about the appropriateness of a communication, the Director of Information Technology or Director of Human Resources or direct Department Head should be consulted.

209.2.7 INTERNET

(a) City Internet facilities are for City-related purposes only. The City Manger's office shall have the final review as to the appropriateness of material and usage of the Internet.

(b) City departments shall use the City's Internet home page for all Internet postings and shall not initiate new or separate services outside of the City's designated services.

(c) Access to the Internet and use of its capabilities to produce or transmit data is not considered private or confidential. Information produced through use of the City Internet system, either in hard copy or electronic format, is considered City property and may be accessed and reviewed without prior notice by the City.

(d) The Information Technology Department has technical responsibility for setting up and managing Internet resources.

(e) Information regarding Internet sites accessed by employees may be considered public information. Access to all sites on the Internet, by any of the staff, is recorded and is subject to review. Access to and/or use of sites that is deemed to be non-City related may result in disciplinary action as described in the City Personnel Rules and Regulations.

(f) When using the Internet no programs or executables should be downloaded without permission from the Information Technology Department. All such files must be scanned for possible viruses. Programs often make changes to desktop systems which conflict with other City software. No software is to be loaded on City desktops without permission from Information Technology.

209.2.8 INTRANET

City Intranet facilities are for internal communications purposes only. The Information Technology Department provides capabilities on the Intranet to post information to be shared between employees. Technology Services will be responsible for reviewing such postings to insure they meet with all aspects of this policy. In the event that concerns develop, the Director of Human Resources will have final editorial authority for Intranet postings.

209.2.9 SOFTWARE

(a) Each piece of software operating on City property shall have a valid registration and be covered by a valid licensing agreement. Software and its associated documentation are covered by Copyright Laws and subject to licensing agreements. Appropriate documentation to substantiate the legitimacy of the licenses shall be forwarded to and kept on file in Information Systems.

(b) Unauthorized or unlicensed software will not be used on City systems.

(c) Authorization to use software on City systems shall be obtained from Information Systems Manager. If approved, Information Systems will either authorize the individual to install the software or install the software for the person, at Information Systems discretion.

209.3 PHONES

(a) All City related telecommunications devices, regardless of type (land line or wireless cell phone) are provided as a tool to conduct City business. The City expects that all such devices will be used in a responsible manner.

(b) Lost cell phones will be replaced once based on if loss is determined to be reasonable by the appropriate Department Head. The City will replace old, outdated or non-functioning cell phones.

(c) Calls to user pay phone numbers (e.g. 900,976) are prohibited unless absolutely necessary for purposes of contacting vendor company help lines. These requests should come through the Information Technology Department. Every attempt has been made to block these numbers through the desk top telephone system.

209.4 CONDITIONS OF CITY ACCESS/PRIVACY

The City places high value on confidentiality. There are nonetheless circumstances in which the City may determine that certain broad concerns outweigh the value of a User's expectation of privacy. All employees, volunteers and elected/appointed officials are to keep in mind that the City's technology resources and all the information contained therein are properties of the City and that no employee should have expectation of privacy regarding the information on the City's computer system.

Employees should be aware that any technology media or communication involving the City's technology resources are considered at all times to be City records. They may be considered public record and be subject to disclosure under the California Public Records Act, Government Code section 6250 et. Seq., or other lawful requests regardless of designations of "private" or "confidential". The City shall comply with all lawful requests for information and shall not be held liable for such lawful disclosure in any manner. Electronic media is also subject to the provisions of the Brown Act and all electronic discussions between elected officials must follow the Brown Act guidelines.

Although the City does not read and review electronic files on a routine basis, the City has the capability to access, monitor, and review, copy and/or disclose any electronic media communications. The City also employs technology to screen electronic communications for such things as viruses or access to inappropriate web sites.

The City reserves the right to do so this for any proper City purpose in accordance with the Electronic Communications Privacy Act of 1986. The City may make backup copies of electronic files. This means that files may be restored, even if the user believes the files have been deleted. An individual's use of technology or electronic media is consent for the City to act accordingly.

209.5 ENFORCEMENT

Violations of this policy will result in disciplinary action as described in the city personnel rules and regulations.

209.6 POLICY DEVELOPMENT

This policy may be periodically reviewed and modified by the Department of Information Technology, who may consult with relevant Departments, Committees, Council, and staff.