ADMINISTRATIVE PROCEDURE	**AP 2-1** Category: Information Technology
	Department: Information Technology
TITLE: Computer Policy – Acceptable Use	Approved: December 7, 2007

A. Overview

1. The Information Technology Department (IT) is committed to protecting City of Peoria's employees, partners and the City from illegal or damaging actions by individuals, either knowingly or unknowingly. The enterprise network and Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, and network accounts providing electronic mail, web browsing, and file transfer capability are the property of City of Peoria. These systems are to be used for business purposes in serving the interests of the City, and of our clients and customers in the course of normal operations.

2. Effective security is a team effort involving the participation and support of every City of Peoria employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

B. Purpose

The purpose of this policy is to outline the acceptable use of computer systems, which include hardware, software, and services, at City of Peoria. These rules are in place to protect the employee and City of Peoria. Inappropriate use exposes City of Peoria to risks including virus attacks, compromise of network systems and services, and legal issues.

C. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at City of Peoria, including all personnel affiliated with third parties. This policy applies to all computer systems that are owned, leased, contracted, or otherwise used in the course of City business by the City, including employee-owned computing devices only when connected to City of Peoria computing resources.

D. Policy

1. General Use and Ownership

a. Users should be aware that the data they create on the city systems remains the property of City of Peoria. Because of the need to protect City of Peoria's network, management cannot guarantee the confidentiality of information stored on any network device belonging to City of Peoria.

b. Employees should not engage in personal use of City information systems, which results in a detrimental impact on the City. Employees should be presuming that personal use other than minimal amounts might result in a detrimental impact on the City. The department head in Information Technology Department shall determine detrimental use.

c. For security and network maintenance purposes, authorized individuals within City of Peoria may monitor equipment, systems and network traffic at any time, per *Information Technology Department's Audit Policy.*

d. City of Peoria reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2. Security and Proprietary Information

Password’s must be kept secure and NOT be shared with other users. Authorized users are responsible for the security of their passwords and accounts. Application passwords should be changed quarterly, network passwords will expire every 60 days and must be changed.

a. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with Paragraph H, “Laptop Security Tips” below.

b. Postings by employees from a City of Peoria e-mail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of City of Peoria, unless posting is in the course of business duties.

c. All hosts used by the employee that are connected to the City of Peoria Internet/Intranet/Extranet, whether owned by the employee or City of Peoria, shall be continually executing approved virus-scanning software with a current virus

database.

d. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malicious programs (e.g. viruses, e-mail bombs, Trojan horse code, etc). If unsure of the content of the attachment, the attachment should be saved prior to opening it.

3. Unacceptable Use

a. The activities listed in paragraphs 4, 5, and 6 below are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

b. Under no circumstances is an employee of City of Peoria authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City of Peoria-owned resources.

c. The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

4. System and Network Activities

The following activities are strictly prohibited:

a. Violations of the rights of any person or city protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by City of Peoria.

b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which City of Peoria or the end user does not have an active license.

c. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Users should consult the Office of the

City Attorney prior to the export of any material in order to determine whether export is permissible.

d. Knowingly introduce malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

e. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

f. Using a City of Peoria Information Systems asset to obtain and/or transmit material could create a hostile and offensive workplace or a sexually charged workplace in violation of Title VII of the Civil Rights Act of 1964 as amended or the Arizona Civil Rights Law.

g. Making fraudulent offers of products, items, or services originating from any City of Peoria account.

h. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

i. Port scanning or security scanning is expressly prohibited unless it is performed by Information Technology Department staff for authorized business purposes.

j. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

k. Circumventing user authentication or security of any host, network or account.

l. Using remote desktop control functionality without IT authorization and approval.

m. Interfering with or denying service to any user other than on the employee's own device (for example, initiating a denial of service attack).

n. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the

Internet/Intranet/Extranet.

o. Providing information about, or lists of, City of Peoria citizens or employees to parties outside City of Peoria unless this activity is part of the employee's job duties.

5. E-mail and Communications Activities

a. The following is a summarized list of prohibited use. Please see the *Internet and E-mail Policy* for more detailed information.

b. Any form of harassment via e-mail, voicemail, telephone or paging, whether through language, frequency, or size of messages.

c. Mass mailing of e-mail "junk mail" or non-city business related advertising material to individuals who did not specifically request such material (e-mail spam).

d. Solicitation of e-mail for any other e-mails address, other than that of the poster's account, with the intent to harass or to collect replies.

e. E-mail posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

6. Unauthorized use or forging of e-mail header information

Use of the City's Information Systems to engage in threatening, intimidating or harassing conduct including but not limited to constituting the alleged harassment that constitute threats, intimidation or any other kind of act that interferes with the individual's ability to function as an employee of the City.

E. Confidential Files

Any files that contain confidential information of City of Peoria citizens or employees will be preserved to contain the confidential information, and the files will not be accessed by IT or anyone else until permission to do so has been granted by a person having authority to do so.

F. Enforcement

1. The City through its department heads and Information Technology Department reserves the right to review an employee's use of city provided information technology services, such as but not limited to, Internet, LAN, on-line services, telephone and e-mail use to determine whether the system's use is appropriate and conforms to this policy.

2. If an employee is found to be not conforming to the sections of this policy, the department director or the Information Technology Director may remove the employee's access to the city's computer network resources.

3. Any employee who fails to abide by this policy may be subject to disciplinary action up to and including termination.

G. Definitions

1. Local Area Network (LAN): Voice and data network used within the City of Peoria and its facilities.

2. "Spam:" Unauthorized and/or unsolicited electronic mass mailings.

H. Laptop Security Tips

1. Never leave your laptop in open view in your car; lock it in the trunk!. But, of course, don't leave it there for any great length of time; exposure to either extreme cold or heat can damage the machine.

2. Always carry your laptop in the provided computer bag or backpack.

3. Never leave your laptop unattended in a public place, including your office. Secure it to your desk at all times, or lock it in a drawer, or "lock-box" even if you leave for a moment. Never leave it unattended anywhere, including residential facilities, unless it is secured or locked away.

4. Never put your laptop on the airport security x-ray machine belt before you have a clear path to the end of the belt.

5. Back up all irreplaceable information daily. Remember, it's not just the loss of the laptop...what about all the hard work and important information that could be lost or stolen.

6. Don't forget to secure all other products associated with your laptop: batteries, power cords, cables, external drives, LCD projectors, etc.

7. Make sure your anti-virus software is up-to-date, and scan your machine for any viruses.

8. Check your laptop computer's battery and make sure it's fully charged. If you take your machine through an airport, the security checkpoint personnel may ask you to turn on the computer to prove it isn't a suspicious device.

9. When traveling, keep your laptop with you at all times, especially while in a public place.

10. Always use your laptop in a cool, dry place.

11. In the event your laptop is lost or stolen, contact the IT Helpdesk immediately to initiate the missing laptop process.

APPROVED:

/S/
Terrence L. Ellis, City Manager

APPROVED AS TO FORM:

/S/
Stephen M. Kemp, City Attorney

Copy Provided to Council: 8/13/02, Issued: 8/23/02 [Prior Numbering: AP 02-03]
Amended Copy Provided to Council: 11/21/07 Issued: 12/07/07