FROM THE OFFICE OF THE MAYOR **ADMINISTRATIVE PROCEDURE MEMORANDUM NO. 3-9**

SUBJECT: APPROPRIATE USE OF CITY COMPUTER RESOURCES

Background: These policies are based on the following premises:

1. Computer resources have become an invaluable asset which must be protected.

2. The City must have a secure, reliable, maintainable and supportable computer network.

3. Unless specifically exempt, information stored in any automated format is considered to be a public record.

4. Software that has not been properly licensed is illegal, and the penalties are severe.

5. Incidental personal use of the City's computer resources by employees strictly in accordance with this APM is permissible.

This APM does not cover employee-owned computers being used for City work. However, employee-owned computers will be stand alone and will not be permanently connected to the City network.

All other Administrative Procedure Memoranda, Madison General Ordinances, and Work Rules governing employee conduct are applicable to the use of City computer resources. These policies shall not be construed to be in conflict with any other City, State or Federal laws, including but not limited to those relating to access to and handling of Municipal Court records.

General Use:

1. All electronic data, communications and information, including information transmitted or stored on the electronic systems of the City, remain the property of the City. The City retains the right to access, inspect, monitor or disclose any material transmitted or received on its electronic systems, including information downloaded from the Internet or received or sent via e-mail.

2. Employees should not expect privacy with respect to information transmitted, received or stored on the City's computing resources. By accepting the grant of access to City electronic systems, the employee shall be deemed to have authorized the City to access, inspect, monitor and disclose material. Consequently, an employee's manager and other authorized individuals shall have the right to know employees' passwords.

3. The Internet and e-mail, whether in-house or external, shall be used in an appropriate and professional manner at all times. The use of language inappropriate to the work place is prohibited. Offensive messages, including racial slurs or sexual slurs, obscene, vulgar and other inappropriate language in violation of APM 3-5 is strictly prohibited.

Incidental Personal Use: Although occasional and limited personal use of computers is tolerated, subject to the limitations, conditions, and regulations contained in this APM, employees may not use any information technology resources in any way that:

- Directly or indirectly interferes with City operations of computing facilities or e-mail services.

- Is contrary to or damages the City's interest.

- Results in any incremental costs to the City.

- Interferes with the employee's work duties, performance or other obligations to the City. Examples include, but are not limited to, excessive use of games, surfing the net, etc.

Any personal use shall be at the risk of the person engaging therein. The City is not responsible or liable for the consequences. Such use shall be limited to individualized personal communications and not mass distribution of material. Using computer resources for incidental personal purposes to transmit material to "all e-mail users" is strictly prohibited. Use of computer resources for such incidental personal purposes is a privilege and can be withdrawn by a supervisor at any time.

Prohibitions and Restrictions On Use: The use of computer resources including the Internet and/or e-mail, whether in-house or external, for any of the following purposes is strictly prohibited:

1. To create or transmit material which is designed or likely to threaten, disturb, intimidate or otherwise annoy or offend another, including, but not limited to, broadcasting unsolicited messages or sending unwanted mail after being advised it is unwanted.

2. To create or transmit defamatory material.

3. To gain unauthorized access to facilities or services accessible by the City network and intended to be used for official City business or to use such facilities or services in an unauthorized manner.

4. To conduct business or engage in any "for profit" communications or activities.

5. To access, view or obtain any "adult entertainment," pornographic or obscene material unless it is for work-related investigatory purposes and with the approval of the department head.

6. For political campaign purposes, including, but not limited to, using e-mail to circulate advertising for political candidates or relating to political campaign issues.

7. Placing one's City-issued Internet e-mail address on any ListServ for other than business purposes. If an employee becomes aware that his/her City-issued Internet e-mail address is on a non-business related ListServ, he/she should promptly request that it be removed and/or unsubscribe.

8. To gain commercial or personal profit or advantage, including, but not limited to, selling lists of names, addresses, telephone numbers or other information generated from City files.

9. To create or transmit material in violation of APM 3-5.

10. To represent oneself directly or indirectly as conducting City business when using such equipment for incidental personal purposes.

11. To create web pages - No personal web pages may be created, regardless upon what server they may reside. Web pages representing official City information may be created in coordination with the Information Services Department.

12. To print lengthy documents except for business purposes.

13. To use the Internet and speakers or headsets for the purpose of listening to audio or viewing video unless it is for City business.

14. For any purpose which would be a violation of any City work rules, City ordinance or state or federal law.

Software: All software running on City computers must be properly licensed and proof of this licensing must be available. Employees may install software licensed to the City on employee-owned computers for work at home only when such installation falls within the licensing agreement with the software vendor and is approved by the employee’s supervisor.

Virus detection software, as recommended by the Personal Computer (PC) Standards Committee, is loaded on all servers and on all PCs. IS will ensure that the virus software is regularly updated.

PC software falls into one of the following three categories:

1. STANDARD SOFTWARE: This is software as defined by the PC Standards Committee, and is fully supported by the IS Department. Any new software that is proposed for City-wide use should first be approved by the PC Standards Committee.

2. OTHER ACCEPTABLE SOFTWARE: This software, while not included in the list of approved PC Standards software, is defined as being of benefit for a particular agency or section. Its use must be approved by the agency head. An important guideline to follow is that there should be a business reason to use the software rather than just personal preference. Support from IS will only be on a “familiarity” basis. Responsibility for such software belongs to the agency where the software is used. Consideration should be given to the possible need to share data created using this software with others.

The minimum hardware configuration, as established in the PC Standards, is more than sufficient to run the Standard Software. If software in this "other acceptable" category should cause the computer's resources, e.g., memory, processing speed, disk storage, etc., to be exhausted, the agency will be responsible for expanding the computer to meet the needs of the software. If this software should have a negative impact on the overall City network, the software may be removed, or the computer may be removed from the network, or the computer may need to be expanded - at the agency's expense.

3. UNAUTHORIZED SOFTWARE: This is software that is not included in either of the above two categories. If any software of this type is found to reside on a City-owned computer, the agency head will be notified and the software may be removed. If this software is running on a networked computer, that computer may be removed from the network until the situation is corrected.

Electronic Mail (Both Internal and Internet) and Access to the World Wide Web and other Servers:

Access to electronic mail (e-mail), both internal and Internet, and access to the World Wide Web is only granted by approval of the agency head.

Transmission of any material in violation of U.S. or state laws or regulations is prohibited.

While the Internet is an effective network for its purpose, it is not and should not be considered a secure network and should not be relied on for the transmission of confidential or sensitive data or messages.

Do not download software to City PCs without authorization from IS. Doing so could put the City in jeopardy of breaking software piracy rules and/or could contaminate the network with viruses.

Attempt to limit the downloading of large files unless absolutely necessary. If it is necessary, try to schedule for off-peak hours (before 7:30 a.m. or after 4:30 p.m.). Remove the files from hard disk when you are finished with them.

Unless approved by IS, do not connect directly to the Internet or to any other external computer system via a PC modem. Employees must use the City's Internet gateways, i.e., Internet e-mail through Group Wise and the World Wide Web through Netscape on the City's network. This is in order to prevent the City's network from being compromised by external factors.

Security and Backup: Employees should take appropriate steps to protect the security of networks and files by the use of passwords and by taking all necessary steps to maintain the integrity of passwords. While managers and supervisors have the right to know employees' passwords, passwords should not otherwise be shared, nor should they be posted. Unless otherwise specifically authorized, viewing any other employee's electronic mail or use of another employee's password without the express permission of that employee is prohibited. E-mail should not be sent to the group "all e-mail users" without the permission of the agency head. If the message is date sensitive, delete it after the date has passed, unless it should be retained under the Open Records Law.

Employees are encouraged to log out of the network or to password-protect their screen savers to avoid security breaches while they are away from their workstations.

Any suspected breach of security should be reported immediately to IS.

IS performs daily backups for all servers attached to the wide area network. Agencies are responsible to insure that backups are performed regularly for hard drives on each PC in their agency. Agencies are encouraged to store critical files on the server (f: drive).

Games: The PCs operating system, Windows, comes equipped with games. The use of these games may allow a new user of a mouse to get the feel of the mouse and to improve hand-eye coordination.

It will be up to the discretion of each agency head as to whether the games that come with the PC should be removed or not.

No other games are to be loaded to a City-owned PC.

IS will not provide any type of support, e.g., loading, training, or troubleshooting for any games beyond the initial use as a training tool.

Consequences: Failure by a City employee to comply with these policies may result in disciplinary action up to and including termination of employment.

Susan JMBauman

Susan J.M. Bauman
Mayor

APM No. 3-9
November 8, 1999

Previous Revision Date: 1/18/96