Executive Order 97-01
POLICY for Use of Computers, E-Mail & Internet

Murray City Corporation

Original January 1, 1997

Revised January 5, 2005

SUBJECT: **Computer Use**

PURPOSE: This Computer Use Policy establishes policy and procedures to be used by all departments regarding the use of computer technology.

Data are an organizational resource. As such, it must be protected as much or more than any other asset or resource. The intent of having and using such data is to accomplish organizational goals. In regards to access to any computer system, software, data, or information on those systems, **there is no expectation of privacy**. The City reserves and intends to exercise the right to review, audit, intercept, access or disclose any system, data, messages, or mail on any City computer system for any City purpose. The goal of this policy is to be consistent with other City policies regarding protection of City assets and to promote their proper use.

The Department Head is responsible for overseeing employees and is responsible for disciplinary action if necessary. The Information Systems department acts in an oversight capacity to insure system procedures are enforced and adhered to.

1. All employees share in the responsibility to protect City computer resources from physical and environmental damage and are responsible for the correct operation, security, and maintenance of those computer resources.

2. All data, files, programs, application software, documents, E-mail, and any other electronic information stored on any computer system owned by the City are considered City property. This includes programs licensed by the City for its use. As City property, all data, files, programs, application software, documents, E-mail, etc., are subject to inspection for purposes of determining compliance with this and other City policies. Employees shall be required to disclose passwords or other security devices upon request of the Department Head, Director of MIS, City Attorney, or Mayor.

3. Software may be loaded onto City computers only if its use has been approved by the Information Systems Department and (1) it is licensed by the City, or (2) it is licensed to an employee of the City.

4. Software will not be copied from City computers for personal use without written approval from the Department Head and Director of Information Systems. Unauthorized

copying constitutes theft. If employees have questions about needing software copies to work at home, they should consult their supervisor. This software can usually be purchased on State of Utah contracts at a discount. If the City buys such software, it will be City property and must be surrendered to the City upon request or at the end of the use or job. However, even if the employee buys the software, all data remains the property of the City.

5. Computers are not to be used to play games. Any game programs found on any computer system will be deleted immediately and the incident reported to the Department or Division Head.

6. Routine backups of data files, programs, and E-mail that are stored on the central computer system and network file servers will occur as part of the systems administration activities performed by Information Systems.

7. Users are responsible for ensuring that backups are made of data files or programs that may be stored on their own computer systems.

8. Configurations of each work station will be determined first by Citywide policy and then departmental policy. Only within those parameters is personal preference to be exercised. Only Information Systems personnel are authorized to reconfigure systems hardware or software. If unauthorized alterations are found, Information Systems personnel will consult with the person(s) and/or the department using the system to determine a solution. If a mutually agreeable solution cannot be found, Information System will inform the Department Head and may take any appropriate action to restore the standard configuration to an operational status. Information Systems personnel may authorize others to install specific approved systems.

9. If unauthorized data or software is found, the Department Head will be notified in writing and opportunity given to rectify the problem (eg. - purchase of software, etc.). If reported unauthorized data or software problems persist and are not rectified within 90 days, the Information Systems Department may delete such unauthorized data or software from computer systems after notifying the Department Head and Chair of the MIS Steering Committee.

10. Computers or terminals should not be left unattended in a state which affords inappropriate access to records of the City or otherwise compromises security.

11. Individual computer profiles and passwords are initially provided by the Information Systems department at the request of Division or Department managers to employees to provide for appropriate access to accomplish job functions. Employees may change their own passwords by following a procedure specified by the Information System department. Each employee with computer access must obtain and use their own individual security profile and password.

12. Employees shall provide all passwords or encryption keys for all protected hardware, software, or documents, to the employee's supervisor prior to use. Employees shall notify their supervisors of their intent to use any other password or encryption to secure computer systems or documents, and explain how and why they intend to use it. Other passwords or data encryption methods may only be used for the purposes of securing information where the information is part of City business and such passwords or encryption is necessary to protect the information according to City requirements for confidentiality.

13. Profiles and passwords shall not be posted, disclosed, or shared among multiple people. Information Systems personnel may take any appropriate action to insure sufficient security for computer systems and data. Passwords may be disclosed to Information Systems personnel for Information Systems purposes.

14. Employees shall provide any passwords or other types of protection or encryption keys to their supervisor or City Attorney, (or designated representative), immediately on request for City business.

15. It is up to the employees' good judgment, good faith, and responsibility to police their own content of messages and other forms of electronic communication. E-mail, Internet or any form of electronic communication should not be harassing, libelous, threatening, abusive, foul, or obscene.

16. All disks, tapes, or data obtained from **outside** the City computers or networks must be checked for viruses BEFORE they are used in the office. This includes all data obtained by any means or from any source.

17. Unauthorized deletion of any information, data, programs, or software from any computer or computer media is a violation of this policy. Violation of this policy may result in personnel action up to and including termination.

Electronic Mail (E-mail) Use

The City has established the following policy with regard to access and disclosure of E-mail messages created, sent or received by City employees using the City's E-mail system.

The City intends to honor the policies set forth below, but reserves the right to change them at any time as may be required.

1. The City maintains an E-mail system. This E-mail system is provided by the City and its use is reserved solely for the conduct of business by the City and its authorized representatives. Incidental personal use of E-mail is permitted on a limited basis.

2. The E-mail system hardware and licensed software are City property. Additionally, all messages composed, sent, or received on the E-mail system are City properties. They are not the private property of any employee.

3. The E-mail system may not be used to solicit for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

4. The E-mail system may be used to promote City approved activities and fund-raisers such as the Employees Association, United Way, March of Dimes, Muscular Dystrophy, or other uses that may be approved by the Mayor.

5. The E-mail system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability.

6. The E-mail system shall not be used to unlawfully send (upload) or receive (download) copyrighted materials which include movies and music, trade secrets, proprietary financial information, or similar materials. It may be done lawfully if it is specified in the employees' job description or with prior authorization from the Department Head.

7. The City reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, sent, or received over the E-mail system for any purpose. The contents of E-mail properly obtained for legitimate business purposes, may be disclosed within the City without the permission of the employee.

8. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.

9. Notwithstanding the City's right to retrieve and read any E-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any E-mail messages that are not sent to them. Any exception to this policy must receive prior approval by the City Attorney.

10. Employees shall not use a code, access a file, or retrieve any stored information, unless authorized to do so. Employees should not attempt to gain access to another employee's messages without the latter's permission.

11. E-mail (both internal and Internet) may be considered a public record and may be subject to public disclosure in accordance with applicable law.

12. Employees who discover a violation of this policy shall notify their supervisor, Department Head, City Attorney, or Director of Information Systems.

13. Any employee who violates this policy or uses the E-mail system for improper purposes shall be subject to discipline, up to and including discharge.

INTERNET USE

Access to the Internet and the use of Internet technologies have become a common means of conducting business. The openness of the Internet and the demands of employees to gain access to Internet resources emphasizes the need to establish guidelines, educate, and raise levels of awareness for all employees involved with Internet technologies. While much of the emphasis is placed on protecting the City or employee from negative impact of the misuse of the Internet, other important significance is placed on the effective use of the Internet so the City can achieve the benefits it desires and expects.

The primary purpose of Internet access is to support and enhance the information resources and communication capabilities of Murray City personnel, and the appropriate sharing of information with other Internet users.

1. Only personnel authorized by the Department Head may post official material on the Internet in behalf of the City.

2. Postings must not violate any trademark or copyright laws. Any trademarks or copyrighted works used in any City posted materials must be so noted to include proper credit to the holders of the trademark and copyright.

3. City Internet facilities are provided to conduct City business and job related activities. Incidental personal use of the Internet is permitted on a limited basis during breaks, lunch, or after hours. Use of the Internet for personal commercial gain is strictly prohibited.

4. Internet access may be provided on an as-needed basis to be determined by the Division or Department Head. Internet E-mail may be available to employees who have access to the Internet and are trained on the City's E-mail package.

5. Software shall not be uploaded or downloaded illegally. It is a serious federal crime, and includes all copyrighted materials, such as movies and music.

6. All downloaded files must be checked for viruses before use.

7. Services on the Internet must not be accessed illegally.

8. Employees must not access Internet sites with lewd, obscene, or sexually explicit material.

9. Any employee who violates this policy or uses the Internet for improper purposes shall be subject to discipline, up to and including discharge.