

A BILL TO CREATE A RESOLUTION ENTITLED:

“A RESOLUTION OF THE CITY OF CENTRALIA MISSOURI, ADOPTING AN AMENDED FORMAL WRITTEN POLICY CONCERNING THE USE OF CITY PROVIDED COMPUTERS, COMPUTER NETWORKS, INTERNET ACCESS, ELECTRONIC MAIL, VOICE MAIL, AND SIMILAR ELECTRONIC COMMUNICATIONS AND INFORMATION STORAGE SYSTEMS.”

WHEREAS, the City of Centralia, Missouri at times provides its elected and appointed officials, employees, volunteers and contractors with computers, a computer network, and access to the internet in order to more easily accomplish their jobs and exchange ideas and information; and

WHEREAS, the City of Centralia, Missouri may in the future provide to such persons other forms of electronic communications and information storage systems; and

WHEREAS, the computers and access to the City computer network and the internet are City-owned or public-owned tools to assist those officials, employees, volunteers and contractors.

NOW, THEREFORE, BE IT RESOLVED THAT THE Board of Aldermen of the City of Centralia, Missouri hereby adopts the following amended formal written policy concerning the use of City-provided computers, computer networks, internet access, electronic mail (“e-mail”), voice mail, and similar electronic communications and information storage systems :

CENTRALIA POLICY

NO. 14 (Amended 12/19/11)

USE OF CITY-PROVIDED COMPUTERS, COMPUTER NETWORKS, INTERNET ACCESS,
ELECTRONIC MAIL, VOICE MAIL, AND SIMILAR ELECTRONIC COMMUNICATIONS AND
INFORMATION STORAGE SYSTEMS

1. Policy Overview

- A. The information system or information network of the City of Centralia (hereinafter referred to as “City”) is defined as the information system that provides electronic data to be stored, transferred, created, modified, or viewed. The information network includes components of computers, PDAs, laptops, printers, storage media, or any item that would be considered information technology in industry standards. The City recognizes the need to develop a policy to set guidelines for the use of the City’s computers and other information network systems. The purpose of this policy is to protect the reliability and integrity of the City’s information systems. The intent of the policy is to protect City residents, customers, elected and appointed employees, volunteers, contractors, and other users during their use of City-owned computers and information systems. This policy sets rules and regulations that shall be followed. Disciplinary actions, including termination, may occur if this policy is not followed.
- B. Goals of this policy are:
 - (1) Establish guidelines for the end user of the City’s computers, establish management monitoring tools, and advise users of acceptable usage policy
 - (2) Establish guidelines for outside vendor support on existing computer hardware and software.
 - (3) Establish guidelines for proper use of Internet, electronic mail, instant messaging, chat rooms, newsgroups and similar electronic information system venues..

- (4) Provide an outline of existing network and future network goals.
 - (5) Establish guidelines about network security and prevent intrusion of the network.
 - (6) Educate end users about viruses and on the use of anti-virus software.
 - (7) Establish guidelines for proper downloading and installation of software.
 - (8) Establish guidelines for installation of hardware.
 - (9) Establish a replacement program for equipment within information systems (i.e. computers, printers, monitors, and network equipment).
- C. The City Administrator may delegate some or all of the following system management activities: backing up system and user files without examining any user's file; routinely adding and removing user accounts; maintaining access controls; withdrawing access privilege temporarily; changing passwords; reviewing logs of system activity; moving user files to safekeeping to restore normal operations and contacting the user to arrange maintenance; the indiscriminate monitoring of all users' activity; the indiscriminate scanning for improperly licenses software; following up the results of indiscriminate scans or monitoring to determine whether a policy infraction and/or illegal activity has likely occurred. Follow-up may involve examining specific users's files. A user's files may also be examined during an investigation of system faults or problems. Any information gleaned from user files as a result of such an examination shall not be disclosed, unless it is the source of a system problem or unless it indicates activity that breaks a law or a City ordinance, rule, or policy.

2. User Responsibilities

- A. The City of Centralia reserves the right to restrict use of its information network components. Such restriction may apply to (but is not limited to) elected and appointed officials, employees, volunteers, contractors, and other users. Consistent with State and Federal Law, the City reserves the right to review all information entered into the information network and to remove or limit access to material posted on or transmitted by its network. Software, files, materials, and data stored on or transmitted by City network are considered the property of the City. All persons using the City-owned computers or computer networks, are advised that they have no personal right to privacy and that no privacy is guaranteed in City-owned or City-provided computers and other communications or data storage systems, including deleted or erased material.
- B. Individual users of City-owned or City-provided computers or other electronic communication or information storage systems shall be held fully responsible and accountable for their communications over and use of such equipment and systems. Users must consider carefully how their computer use will affect other users and whether their behavior is prohibited under City ordinance, rule, or policy or under State of Federal law. Users of City-owned or City-provided information systems are expected to practice civility and courtesy during that use.
- C. Violations of State or Federal law shall be reported to the appropriate authorities, while violations of City ordinance, rules, or policies shall be subject to the appropriate disciplinary process (to include immediate termination). Remedial interventions or educational processes prior to or during disciplinary response may be initiated by the City Administrator or his designated representative, but such interventions will not preclude disciplinary action. Internet or systems access may be restricted or deactivated to an individual, if necessary and in the opinion of the appropriate department head or City Administrator.
- D. Users of City information systems shall respect intellectual property which resides on or is accessed through City information systems and refrain from using the intellectual properties of others. Illegitimate use of such property includes, but is not limited to, unauthorized downloading, copying, or use of software programs (applications) without express permission or license by and from the owner, unauthorized reproduction or posting of copyrighted

material, unauthorized use of trademarks or other protected symbols, and the use of programs and written or recorded materials, or parts thereof, as one's own without acknowledgment of the owner/author.

- E. Computer systems users shall be responsible for knowing and abiding by policies concerning access to passwords, fraudulent, or unauthorized use of systems and installation for access and use of files and systems. All users shall comply with the use requirements (acceptable use policies) of other networks traversed. Use requirements (acceptable use policies) are generally available for each such network. Some source programs, applications, or systems are provided to the City by contracts or licenses; therefore, users shall abide by the City's software contracts and by the City's own policy and shall not copy programs or systems for personal use.
- F. Users are required to save City-related items to corresponding folders on the network drive. City-related items shall not be saved to the local drive (C:) or on portable data storage media (PDAs, disks, USB memory keys, etc.). Except for duplicate copies of an employee's own work product, which may be made to enable users to accomplish City work at home or on non-City computers, saving City-related items on other data storage media or to drives other than the network drive may result in disciplinary action up to termination.
- G. Before leaving work users of a City computer system shall log out and turn off the computer monitor; the CPU may be left on. Printers shall be left on at all times to serve the needs of network users who may be working during off-hours.
- H. The Chief of Police shall retain copies of software contracts and licenses and provide the originals to the City Administrator for proper records retention. The Chief of Police shall provide the original copies of software installation media and instructions to the City Administrator for secure retention. The Chief of Police shall provide the City Administrator with copies of any other policies concerning computers, computer systems and other electronic media adopted for his department and of any other information which might bear on the proper operation, maintenance, or administration of general City-owned computers, computer systems, and other electronic media.

3. General Prohibitions

A user who violates any of the following prohibitions will have network access restricted and/or the privilege revoked and such violations may result in disciplinary action up to termination.

- A. All passwords shall be personal passwords and shall not be given to others. Passwords must conform to current security practices.
- B. No person shall use City-owned or City-provided computers, computer networks, internet access or other City-provided electronic communications or information storage systems for the theft of telephone or communications services; to facilitate unauthorized access to telephone or communications services; to perpetrate fraud, theft, misrepresentation or any other illegal activity or purpose; or to commit any act chargeable as a violation of Federal, State or local law, whether or not charges are brought by authorities.
- C. No person shall use City-owned or City-provided computers, computer networks, internet access, or other City-provided electronic communication or information storage systems in such a manner as to violate any City or departmental rule or ethical standard.
- D. No person shall use City-owned or City-provided computers, computer networks, internet access, or other City-provided electronic communication or information storage systems for personal commercial or business purposes or personal financial benefit.
- E. No person shall use City-owned or City-provided computers, computer networks, internet access, or other City-provided electronic communication or information storage systems to send obscene, pornographic, sexually explicit, threatening, or harassing messages of any kind. In the case of sexual harassment, such messages shall be reported as required by the City's sexual harassment policy. If possible, copies of the offending materials shall be made

- and preserved for review by the department head or other City authorities.
- F. No person shall use City-owned or City-provided computers, computer networks, internet access, or other City-provided electronic communication or information storage systems to search for, find, access, or download any obscene, pornographic or sexually explicit material, except for authorized governmental purposes.
 - G. When using City-owned or City-provided computers, computer networks, internet access, or other City-provided electronic communication or information storage systems, no job names, notes, codes, or file names shall be used that could be construed as racial, sexual, religious, or ethnic slurs.
 - H. No person shall use City-owned or City-provided computers, computer system, or network in an unauthorized attempt to access administrative data on any other City computing network, or to obstruct any City research, administrative, disciplinary, or work activity or to disrupt computer network traffic by recklessly or intentionally overloading the system or otherwise denying or restricting the access of others. No person shall use City computing resources in an extravagant or wasteful manner or in a manner unrelated to bona fide City administrative, research, or instructional purposes.
 - I. No person shall send a message in such a way that it appears to be sent by another person or use a computer system or network anonymously or use pseudonyms to attempt to escape from prosecution of laws or regulations, or otherwise escape responsibility.
 - J. No person shall use City computing network to initiate or encourage the promulgation of chain letters, unauthorized automated or mass postings, or other types of unauthorized large-scale distributions.
 - K. No person shall circumvent or attempt to circumvent City computer network security systems or use City computer systems or networks to circumvent security systems elsewhere; nor shall any person use City computer systems or networks to eavesdrop or collect passwords or other authentication information.
 - L. No person shall use City computing network to copy, download, use, possess, or cause to be copied for use computer software data, data processing equipment or computer accounts without authorization. All copyrights and proprietary rights in computer software or data shall be respected. No person shall place or cause to be placed into public locations proprietary computer software in any form unless specifically allowed by its owner. Such locations include, but are not limited to, file servers, non-private computer files, or folders and computer bulletin boards.
 - M. No person using City computing facilities shall divulge a City computer account password to anyone other than the person to whom the account is assigned, provide others with access to a user's personal computer password(s), or gain or attempt to gain access to the personal computer files or electronic information of others or to files or systems to which authorized access has not been granted. Further, when accessing administrative or other computer data, every person shall take care to protect the confidentiality of the information and respect the privacy of the individuals to whom the information refers.
 - N. No person shall knowingly alter, delete or destroy data, information, or program instructions contained on or in a computer, computer system, computer network, information storage media, or peripheral equipment without the consent of the author of such data, information, or program instructions, or the City Administrator (or Chief of Police for data, information, or program instructions under the control of the Police Department).
 - O. No person shall knowingly introduce a set of instructions, program or otherwise, in a City computer, computer system, computer network, information storage media, or peripheral equipment that will cause a computer, computer system, computer network information storage media or peripheral equipment to do things unwanted by the City.
 - P. No person shall create, on City or City-related premises, or using property belonging to the City, a set of instructions, program or otherwise, that will cause any computer, computer system, computer network, information storage media, or peripheral equipment to do things

- unwanted by the owners thereof.
- Q. No person other than the City Administrator, or his authorized representative (or the Chief of Police where applicable) shall intentionally cancel another's posting to electronic bulletin boards, news groups, etc, or revise or remove any authorized postings on a City web site. For electronic bulletin boards, news groups, or web sites created or controlled solely by the Police Department, such authority shall rest with the Chief of Police.
 - R. No person shall knowingly connect, disconnect, tamper with or make changes to any physical components of a City computer system or computer network other than the person to whom such duties are delegated by the City Administrator, or his designated representative (or the Chief of Police, where applicable.).
 - S. No person shall use or allow use of a City computer account by someone other than the owner to whom the account has been assigned by the City, even if the owner has given permission to the other person, except for group accounts for which valid City access authority has been obtained. All owners of computer accounts shall notify the City Administrator, or his designated representative (or the Chief of Police, where applicable) if they suspect anyone else has used their account.,
 - T. No person shall use a City computer account after that person's employment or contractual association with the City ends.
 - U. No person shall use City-owned or City-provided computers, computer networks, internet, internet access, or other City-provided electronic communication or information storage system for other than incidental personal use in such a manner as to be substantially detrimental to the person's job duties and work time, or create an actual cost to the City as determined by the City Administrator or appropriate department head.
 - V. Uses and actions otherwise prohibited above shall not be prohibited when performed by police or other personnel when in the lawful conduct of their duties and legitimate functions of the City. (For example, the access of pornographic or sexually explicit material and storage thereof is not prohibited when such is a part of a lawful investigation or the maintenance of evidence.)
 - W. No person shall use City-owned or City-provided computers or other electronic communication or information storage systems in any way that hinders work performance, efficiency or production. In the opinion of the City Administrator, Police Chief, or Department Head These include, but not be limited to, games, Internet, chat rooms, non-city related email, and downloading software.
 - X. No person shall inappropriately reveal confidential City information, customer data, or any other material which has been deemed to be a closed record, without the permission of the custodian of records (City Administrator).
 - Y. No person shall change their system configuration or take other steps to defeat any virus protection on a City-owned computer system. No person shall without written permission of the City Administrator add additional security to a workstation or files. Users who believe they have security needs that go beyond current City standards and tools should contact the appropriate systems manager.

4. Outside Vendor Responsibility

From time to time the City of Centralia requires support from outside (external) vendors. This is necessary to maintain up-to-date hardware, software, and security. Such vendors shall abide by the following rules.

- A. Outside vendors shall contact the City of Centralia's network administrator or City Administrator before working on any City-owned or City-provided information system.
- B. Outside vendors shall follow this policy.
- C. Outside vendors shall maintain the protection of any network or user password needed for support. Upon completion of the job, vendors will consult with the network administrator or City Administrator to determine whether any system or personal passwords need to be

- changed.
- D. Outside vendors shall explain the reason for support and what was done to information systems to necessary City staff.
- E. Outside vendors shall contact the City of Centralia network administrator or City Administrator upon completion of support work.

5. Internet

Internet usage is allowed on City of Centralia computers. Internet usage is highly encouraged to improve policies and efficiency of the City departments. It is City policy not to discourage use of the internet or “surfing the web”. Users shall use the Internet to better the City, community, and themselves. However, if the use of the Internet hinders or interferes with individuals doing their primary job, disciplinary action can be administered. The City does not use filtering software to identify inappropriate web sites, but reserves the right to obtain and use such software if it becomes necessary. If the user has connected to an inappropriate site, it is the user’s responsibility to disconnect immediately. Any software or freeware downloaded via the Internet into City computers become the property of the City. All files, and software applications shall be used only in ways that are consistent with licenses and copyrights. When using the internet:

- A. No user may use City computers to knowingly download or distributed infected software or data.
- B. No user may use City computers to knowingly propagate code of malicious or destructive methods (i.e. viruses, worms, or Trojan Horses).
- C. No user may use City computers to knowingly disable or overload any computer system or network or to circumvent any system intended to protect the privacy or security of another user.
- D. All users shall identify themselves honestly, accurately, and completely when participating in chats or newsgroups when using City computers.
- E. Only users who are City-authorized to speak to the new media, or in public gatherings on behalf of the City may speak or write in the name of the City to any chat room or newsgroup.
- F. The City retains the copyright to any external posting to any forum, newsgroup, chat or web page by any employee in the course of duties.
- G. Users are reminded that chat rooms and newsgroups are public forums; users shall no reveal City information, customer data, and other material that are closed records.
- H. Use of City computers to conduct improper activities such as misuse of assets or resources, sexual harassment, unauthorized public speaking, and misappropriation or theft of intellectual property shall grounds for discipline.

6. Email, Chat Rooms, Newsgroups, Podcasts, RSS, and XML Feeds

- A. Electronic mail (email) is provided for all employees of the City. Users may obtain their email address from the City’s network administrator. Email is a communication tool and should be used in that manner. Email messages are the property of the City and can be received by the City. All data stored may be subject to government data procedures studies which make the data accessible to the public; therefore, sensitive or personal messages shall not be sent by email.
- B. Unchecked or stored email and podcast downloads can be a burden to a computer system. Users shall check their email often and remove messages that are no longer needed. Users shall avoid long-term storage of downloads and files obtained from podcasts, chat rooms, newsgroups, and similar systems unless such storage is required by open records regulations or has a clear City purpose.

The following shall be followed:

- (1) Chain emails are not allowed on City computers. Mass emails are not allowed on City computers except when clearly required for communication of City business to all City employees and departments .
- (2) Delete or stored on permanent storage media email messages older than one year. (Authorized City personnel may delete all electronic mail located in mail holding areas after one year.)
- (3) Do not open attachments that are unexpected.
- (4) Do not forward or send emails that are suspected or known to contain malicious code.
- (5) Users may check email from locations away from City facilities, but shall always follow the provisions of this policy and shall always maintain good security practices.

7. Security

- A. At all times it will be both the City's and the user's responsibility to maintain protection of network components from malicious attacks, internal and external.
- B. Individual passwords are the individual's responsibility to maintain and keep private.
- C. Except for individual work project in progress which are stored on transportable media, all data shall be stored on a City-owned or City provided network. The network does not always back up workstation hard drives (the "C" drive). Also the process of reconfiguring workstations as the network environment changes may at any time result in the loss of data stored on a workstation's hard drive. Users of City-owned computers and networks are responsible for backing up their data and computer software from their "C" drive to the network servers or their own storage media. Whenever possible, all users are responsible for deleting outdated files, except those which must be retained under state statute or regulation..
- D. To facilitate off-site work, employees may copy appropriate files to and from storage media. Appropriate files include word processing documents, electronic spreadsheets, and presentation graphic files (for example, files created in Word for Windows, Excel, or PowerPoint). No other files or information may be copied from or to the City computer network or City-owned computes or information storage systems without prior written consent.

8. City-owned Portable Computers

The City owns portable or laptop computers for employee use for City business. The following conditions shall be adhered to when such computers are taken from City premises by City employees:

- A. The portable or laptop computer and accessories shall be signed out by an individual, who becomes solely responsible for it.
- B. Items signed-out shall be returned in good working order and undamaged, with no corrupt data or malicious code.
- C. The laptop computer used by the City Clerk to record minutes for the Board of Aldermen shall be returned to City Hall by 9:00 a.m. of the Friday proceeding the next meeting of the Board of Aldermen (usually the third Monday of every month). This computer may be re-signed out following the meeting.

9. PDA's

- A. Personal handheld computers (PDA's) may be connected to the City network.
- B. PDA software and sync managers shall be approved by the network administrator before installation on desktop computers.

10. Compliance Reviews

The City shall perform periodic and random compliance reviews, which may include the following:

- A. Comparing software inventory records to physical inventory
- B. Reviewing physical storage of original, licensed software disks
- C. Reviewing employee awareness and recognition of this policy
- D. Reviewing software purchasing, inventory, and controls

Reviews shall be conducted at least annually by the City Administrator or his or her designated computer administrator(s); except for assets of the Police Department, which shall be reviewed by the Chief of Police or his or her designated computer administrator(s). Results of reviews conducted for the Police Department shall be copied to the City Administrator. Prior to reports being submitted, the reviewing parties shall compare reports to be sure that installation and use of “shared” software is in compliance with the number of users allowed by each software license. When additional licenses must be purchased, the expense for such additional licenses shall be charged to the department necessitating the additional users.

11. Forms

The City Administrator shall create the following forms for use by City employees:

- A. Request for software or hardware installation. This form shall be filled out and returned to the City Administrator or City network administrator before installing any software, application, or hardware component to the City network.
- B. User Acknowledgment. This form shall be filled out and returned to the City Administrator or City network administrator by any employee, official, or contractor to first activate a City account (username and password). This form shall be returned 14 days after the user’s hire date or appointment date or after adoption by the Board of Aldermen of any amendment of this policy. Failure to return the form will result in the City account being not turned on or deactivated.

12. Replacement Policy of City Information Technology Infrastructure

- A. The City shall replace one-fifth of the City computer (computer processing unit) inventory on a yearly basis. Network items such as hubs, routers, and cable shall be replaced on an as-needed basis. Computer monitors and printers shall be replaced as needed, but not less frequently than every ten (10) years. The annual budget shall reflect such replacement purchases.
- B. When any City Computer is to be sold, given away, or otherwise leaves City ownership or control, the hard drive shall first be removed and physically destroyed. If the hard drive cannot be removed from the rest of the computer, then the entire computer shall be destroyed in a manner that renders any stored information permanently irretrievable.

13. Policy Review

This policy shall be reviewed by the City Administrator at least biannually. The Mayor, City Administrator, or Chief of Police where applicable, may on a case-by-case basis temporarily waive provisions of this policy when such waiver is by their judgement in the best interests of the City. Any waiver or change a recurring or general nature shall be referred to the Board of Aldermen for possible amendment of this policy.

PASSED AND APPROVED this 19th day of December, 2011.

Mayor

ATTEST:

City Clerk

G:\LYNN\ARCIVE08\POLICYCMPTRUSE5.res.wpd