



**CITY OF LODI
COUNCIL COMMUNICATION**

TM

AGENDA TITLE: Adopt resolution concurring with staff recommended Network Access and Acceptable Use Policy

MEETING DATE: December 17,2008

PREPARED BY: Information Systems Manager

RECOMMENDED ACTION: Adopt resolution concurring with staff recommended Network Access and Acceptable Use Policy.

BACKGROUND INFORMATION: The health and safety of the City's computer assets and infrastructure largely depend upon network security. Without an appropriate policy, the availability of the City's network can be compromised through intentional and unintentional use. The purpose of this Policy is to establish the rules for access and use of network resources, in addition to defining certain procedures for maintaining a secure network.

With the use of computer networks comes the real threat of damage and liability when unauthorized access occurs or misuse of network computer assets happens. Networks also increase the exposure to computer viruses and other malicious utilities.

The attached policy has been the City's standard of practice since July 2006; however, the 2008 audit revealed the practices had not been formally adopted by the City Council.

This policy addresses user access rights, password standards, directory management, appropriate use and prohibitions, network maintenance and backups, among others.

Staff recommends adoption of a resolution concurring with the proposed Network Access and Acceptable Use Policy in order to help ensure the safety and security of the City's networks and computer assets.

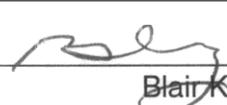
FISCAL IMPACT N/A.

FUNDING: N/A

Respectfully Submitted,



Steve Mann
Information Systems Manager

APPROVED:  _____
Blair King, City Manager

RESOLUTION NO. 2008-247

A RESOLUTION OF THE LODI CITY COUNCIL
APPROVING THE NETWORK ACCESS AND
ACCEPTABLE USE POLICY

WHEREAS, the health and safety of the City's computer assets and infrastructure largely depend upon network security; and

WHEREAS, without an appropriate policy, the availability of the City's network can be compromised through intentional and unintentional use; and

WHEREAS, with the use of computer networks comes the real threat of damage and liability when unauthorized access occurs or misuse of network computer assets happens; and

WHEREAS, computer networks also increase the exposure to computer viruses and other malicious utilities; and

WHEREAS, the purpose of this Policy is to establish the rules for access and use of network resources, in addition to defining certain procedures for maintaining a secure network; and

WHEREAS, staff recommends adoption of a resolution approving the Network Access and Acceptable Use Policy in order to help ensure the safety and security of the City's networks and computer assets.

NOW, THEREFORE, BE IT RESOLVED that the Lodi City Council hereby adopts the Network Access and Acceptable Use Policy.

Dated: December 17, 2008

I hereby certify that Resolution No. 2008-247 was passed and adopted by the City Council of the City of Lodi in a regular meeting held December 17, 2008, by the following vote:

AYES: COUNCIL MEMBERS – Hitchcock, Johnson, Katzakian, Mounce,
and Mayor Hansen

NOES: COUNCIL MEMBERS – None

ABSENT: COUNCIL MEMBERS – None

ABSTAIN: COUNCIL MEMBERS – None


RANDI JOHL
City Clerk

SUBJECT: NETWORK ACCESS AND ACCEPTABLE
USE- Policy

DATE ISSUED: DECEMBER 17,2008

SECTION: A

SECTION 1: PURPOSE

To ensure appropriate management of the City of Lodi's local and wide area network systems by controlling access, promoting consistency in use, and providing administrative functions to support the business of the City.

SECTION 2: POLICY

This Policy applies to all individuals who have been provided access rights to the City of Lodi networks, City-provided email, and/or Internet via agency-issued network or system User ID's

1) General

- a) Use of the City of Lodi's network shall be in accordance with all applicable rules, regulations, and policies.
- b) All network systems and information created on, stored within, or transferred from or to other media (floppy disk, tape, CD) are, and shall remain, the property of City of Lodi, subject to its sole control.
- c) Users shall be given Limited User Rights (rights govern access to local and network resources) on their local PC; local administrative rights shall only be issued when approved by the Information Systems Manager or Network Administrator, or their designee, when circumstances warrant
- d) Virtual Private Network (VPN) access shall be granted only upon completion of a properly signed and executed VPN Acceptable Use Agreement and as approved by the Information Systems Manager or Network Administrator.
- e) IBM user accounts shall be issued only upon completion of a properly signed and executed User Access Application.

9 The City Manager reserves the right to interpret this policy.

2) Access to City of Lodi's Network

- a) City of Lodi employees shall be assigned a user account for the duration of employment within the City of Lodi. It is the responsibility of an employee's supervisor to file requests to add, modify, or delete network accounts via the City's Helpdesk system.
- b) Contract employees shall be assigned a user account when appropriate. The City of Lodi supervisor responsible for contract management shall file appropriate requests to add, modify, or delete a user accounts.

3) Network Accounts and Passwords

a) Users shall be issued a network logon consisting of a **username** and temporary password. The **Username** shall include the first initial of the user's first name and as much of the last name as possible, expressed together as one word or contiguous string, e.g., "jdoe." The user's middle initial may also be used in the case of two users with the same name.

b) Passwords shall meet the following minimum standards:

- Passwords will expire every 90 days, at which time a new one must be created
- **Users** may change their passwords more often, if desired
- The system will prompt users to change passwords as they expire
- Password changes may be made from your computer
- The same password cannot be used until at least four unique passwords have been used
- Passwords must be at least six characters in length
- Passwords must contain characters from at least three (3) of the following four (4) classes:

Description	Examples
Upper case letters	A, B, C, ... Z
Lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric ("special characters") such as punctuation symbols (# (&))	

- Passwords may not contain the user's name or any part of their full name (password cannot be "Bill#1" if your name is Bill Smith).

c) Regular password changes are also required for IBM AS400 users:

- Passwords will expire every 90 days
- Passwords must start with a letter (e.g., "A", "Z", etc)
- Passwords can be no longer than 10 characters on the AS400
- Special characters may also be used for these passwords

Exceptions to the above standards may be granted in special cases, as approved by the Information Systems Manager, or his designee, or the Network Administrator.

4) Management of Network Directories

A network is a collection of desktop computers and devices that has the ability to electronically communicate between devices and share resources. The City of Lodi's network provides users with additional storage space for data and information in a central, controlled environment. This allows for efficient sharing of data and information as well as secured access and mass backup functions. The network directories shall be managed as follows:

- a) The Information Systems Division (ISD) is responsible for setting up network directories to accommodate sharing of files among users within business defined work units. Directories will be created in such a way as to restrict uncontrolled access. ISD will work with the business units to determine the best sets of shared directories, based upon requirements for efficient sharing and storing of business files and security for that data.
- b) The business units are responsible for designating those users who will be granted rights to access specific directories. Supervisors are responsible for requesting additions, modifications, and deletions to the user list.
- c) Only designated ISD technical staff shall have administrative control rights on the City of Lodi's network in order to support and maintain the system.
- d) Business units are responsible for approving access requests to shared directories for City of Lodi's users outside of the defined work unit. Business units shall forward approved requests to the ISD Help Desk for implementation.
- e) The Information Systems Division shall determine the location of applications files. Installation of software is the responsibility of ISD.

5) Use of Network

Electronic files are stored in locations accessed from the desktop, either locally on the individual desktop hard drive (commonly called the C: drive) or in locations referred to as network directories (e.g. P: drive). Each authorized user is provided a network account with access to a personal home directory and to an assigned shared directory. Acceptable use of the network includes:

- a) City of Lodi reserves the right to monitor network use either at random or for cause. Appropriate use is determined by the City of Lodi's Electronic Media Use Policy. Inappropriate use will be subject to loss of account privileges or disciplinary action, up to and including dismissal.
- b) Personal Home Directory:
 - i) Only the named user will have rights to that user's personal home directory.
 - ii) Use of the personal home directory (commonly called the P: drive) for personal files relating to specific job duties (i.e. working drafts, confidential personnel files, etc.).
 - iii) Designated ISD technical staff may obtain access when necessary in their duty of supporting the user of the account.
- c) Shared Directory:
 - i) Only those users or groups of users determined by specific business units shall have rights to designated shared directories.
 - ii) Users should use the assigned shared directory for City of Lodi business files that are accessed, used, viewed, or otherwise shared with other employees (i.e. reports, correspondence, project documents, reference materials, etc.).
 - iii) Designated City of Lodi technical staff may obtain access when necessary in their duty of supporting the user of the account.
- d) Local Hard Drive:

- i) The user of the desktop has access to the local drive. This drive is not necessarily secured from access by unauthorized users.
 - ii) The hard drive (commonly called the C: drive or local drive) should not be used for permanent City of Lodi file storage, as data could be lost in the case of malfunction.
 - iii) ISD does not perform routine backups of the hard drive contents.
 - iv) Designated ISD technical staff may obtain access when necessary in their duty of supporting the user of the account.
- e) Prohibitions
- i) Sending or sharing with unauthorized persons any information that is confidential by law, rule or regulation
 - ii) Installing software that has not been authorized by the respective department head in concurrence with the Information Systems Division
 - iii) Installing or attaching to the City's network any personal or non-city owned devices (e.g. laptops, thumb drives, other computing devices) without the knowledge and approval of ISD and the respective department head
 - iv) Attaching processing devices that have not been authorized by the respective department head in concurrence with the Information Systems Division
 - v) Using network resources to play or download games, music or videos that are not in support of business functions
 - vi) Leaving workstation unattended without engaging password protection for the keyboard or workstation
 - vii) Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing
 - viii) Using network resources in support of unlawful activities as defined by federal, state, and local law
 - ix) Utilizing network resources for activities that violate conduct policies established by the City of Lodi.
 - x) City network resources may not be used to engage in union or bargaining unit activities

f) Network Maintenance

Network storage space is limited. There is an optimal amount of free space at which efficient use and speed of the network occurs for storing and retrieval activities. Users must actively manage the amount of information stored on the network.

- i) Users are responsible for identifying files that are no longer required as determined by their business unit supervisor. Obsolete files should be moved or purged from the network drives.
- ii) Users shall be limited to the following storage limits: **50MB** for email, **75MB** for network files.
- iii) **As** a courtesy to City employees and as a matter of routine, the Information Systems Division shall make and retain backup copies of e-mail messages for a period of 30 days, after which time they will be subject to deletion. Under some circumstances, communications sent by e-mail may be subject to

public disclosure under the Public Records Act or by litigation. E-mail deemed to be public record should be printed out in hardcopy form and kept for a prescribed period of time. As an alternative, subject e-mail messages may be kept in electronic form on the individual user's computer hard drive or on some other storage media (e.g. CD-ROM, Ropyy disk, DVD, etc.) In any case, it is the responsibility of each City employee to determine if a message qualifies for the Public Records Act, and if it does, make provisions for its safekeeping. Messages not deemed to be part of the public record may be deleted at any time by the user.

g) Network Backup

ISD is responsible for establishing a routine backup scheme to copy information from the City of Lodi network directories to a second medium as a precaution in case of network failure.

- i) Network backups will include all network directories, including all personal and shared folders.
- ii) At a minimum, backups will occur daily of all network data files that have been modified or added since the last full, archival backup. These daily backups are kept for short periods.
- iii) Archival backups, backup of all network files, shall occur at least monthly. These full backups are kept for at least one month and may be kept for longer periods, up to and including permanent storage.

h) Local Hard Drive Backup

- i) Users are responsible for all backups of data and information stored on their desktop local drive (C:). Users are encouraged to regularly backup any important files kept on the local drive.

i) Periodic reviews of users and user rights

- i) Information Systems Division shall periodically review the lists of system and application users to ensure that access rights are authorized and up-to-date. Reviews shall be done at least annually and will be performed by submitting a list of users and their respective access rights to department heads for certification. Department heads shall report to Information Systems Division any changes in users or their respective access rights, and Information Systems Division personnel shall adjust in a timely manner the users and user rights as recommended by the department heads. The reviewed lists shall be kept on file by Information Systems Division as documentation of these actions.

j) Statement of Enforcement

- i) Noncompliance with this policy may result in termination of user access, in addition to other disciplinary actions taken by the appropriate parties.