LODI CITY COUNCIL

Carnegie Forum
305 West Pine Street, Lodi

"SHIRTSLEEVE" SESSION
Date: December 14, 2010
Time: 7:00 a.m.

For information regarding this Agenda please contact:
Randi Johl
City Clerk
Telephone: (209) 333-6702

NOTE: All staff reports or other written documentation relating to each item of business referred to on the agenda are on file in the Office of the City Clerk, located at 221 W. Pine Street, Lodi, and are available for public inspection. If requested, the agenda shall be made available in appropriate alternative formats to persons with a disability, as required by Section 202 of the Americans with Disabilities Act of 1990 (42 U.S.C. Sec. 12132), and the federal rules and regulations adopted in implementation thereof. To make a request for disability-related modification or accommodation contact the City Clerk's Office as soon as possible and at least 24 hours prior to the meeting date.

Informal Informational Meeting

A. Roll Call by City Clerk

B. Topic(s)

B-1 Receive Presentation on Information Technology Policies (CM)

C. Comments by Public on Non-Agenda Items

D. Adjournment

Pursuant to Section 54954.2(a) of the Government Code of the State of California, this agenda was posted at least 72 hours in advance of the scheduled meeting at a public place freely accessible to the public 24 hours a day.

_____
Randi Johl
City Clerk

AGENDA ITEM B-01

CITY OF LODI
COUNCIL COMMUNICATION

TM

AGENDA TITLE: Receive Presentation on Information Technology Policies

MEETING DATE: December 14, 2010

PREPARED BY: Information Systems Manager

RECOMMENDED ACTION: Receive Presentation on Information Technology Policies.

BACKGROUND INFORMATION: The City's auditors have included in their prior year's management letter a number of recommendations related to IT changes and improvements. Most of the recommendations relate to internal security and methodologies, which seek to bring City practices into generally accepted industry standards and practices.

The Information Systems Division has worked with the auditors, City departments and employee groups to bring about the desired changes and to have them documented in a series of IT policies. The policies range in scope from governing Internet use to defining how often user passwords shall be changed. The policies are intended to apply to everyone who has access to the City of Lodi's computing and information resources.

Among the highlights are:

- Defines acceptable and unacceptable use
- Network access and acceptable use
- Acceptable uses of social network sites
- Web filtering policies and practices
- Software selection and acquisition
- Change control
- Patch management
- E-waste disposal

Both staff and the auditors feel it is important to set standards and define practices and procedures, and to have them adopted by the City Council, in recognition of the growing importance of and dependence upon technology in the workplace. Adoption of these policies will close out the management letter comments by the external auditors.

FISCAL IMPACT: None

_____
Jordan Ayers
Deputy City Manager/Internal Services Director

Prepared by: Steve Mann, Information Systems Manager

APPROVED: _____
Konradt Bartlam, City Manager

CITY OF LODI
ADMINISTRATIVE POLICY AND PROCEDURE MANUAL

SUBJECT: : INFORMATION SYSTEMS

DATE ISSUED: : DECEMBER 2010

This portion of the Administrative Policy and Procedure Manual defines the policies and procedures applicable to the City's information systems. Primary responsibility for these policies and procedures rests with the Deputy City Manager/Internal Services Director and are administered through the Information Services Division of the Internal Services Department. These policies and procedure apply to all departments, divisions and individuals within the City of Lodi.

SECTION 1: ELECTRONIC MEDIA ACCEPTABLE USAGE

PURPOSE

This policy addresses the acceptable use of Electronic Media[1] at the City of Lodi. These rules are in place to protect the employees and the City. Inappropriate use of Electronic Media exposes the City to risks including computer virus attacks, compromise of network systems and services, and legal issues.

---

[1] For purposes of this policy Electronic Media means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

SCOPE

Anyone using the City of Lodi's computing and information resources is expected to act in a responsible manner by complying with all policies, relevant laws, and contractual agreements related to computers, networks, communication equipment (such as telephones, cell phones and radios, software), and electronically stored or generated information.

This policy applies to anyone who has access to the City of Lodi's computing and information resources, which includes City employees (full-time and part-time), contractors, consultants, temporary employees, volunteers, and elected and appointed officials. This policy also applies to all equipment that is owned or leased by the City or personal equipment that is connected to, networked, or used to read or transmit Electronic Media that contains information that originated from City information systems.

In recognition of the diverse nature of some Police Department activities related to investigations and also Library staff to comply with the Child Internet Protection Act – and by extension Information Systems Division as they may be called upon to investigate alleged violation of these policies – exception to these policies as it relates to storage and/or access to sexual materials may be granted with the approval of the Police Chief and Deputy City Manager, respectively. In all cases, the respective department heads shall be ultimately responsible for oversight and ensuring that exemptions are being used for their intended purposes.

DESCRIPTION

Management's commitment is to protect the City's employees, volunteers, vendors, partners, and the organization from illegal or damaging actions by intentional or unintentional means.

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts that provide electronic mail, Web browsing, and file transfer protocols, are the property of the City. These systems shall be used only for authorized City business purposes in serving the interests of the organization and the public in the course of normal operations.

Effective security is a team effort involving the participation and support of every City employee and affiliate who deals with information and/or information systems. Every user of Electronic Media is responsible for knowing the content of this policy and conducting their activities in compliance with it.

GENERAL USE AND OWNERSHIP

While the City's Information Systems administrators desire to provide a reasonable level of privacy, users should be aware that the data they create on the City systems remains the property of the City. Because of the need to protect

the City's network, management cannot guarantee the confidentiality of information stored on any network device owned, leased or controlled by the City, medical and criminal data stored on secure City systems notwithstanding.

Department heads have ultimate accountability for subordinate compliance of acceptable use policies and responsibility to ensure that the use of technical resources is consistent with the business and service purposes of the department. Anyone provided access to the City of Lodi's computing and information resources has the responsibility to understand and comply with these policies.

The Information Systems Division (ISD) assumes responsibility for the policies herein contained, as follows:

Resolve issues where compliance with these policies conflict with those imposed by State or Federal agencies on City departments and agencies.

Work as requested with departments and others to ensure a solid understanding of these policies.

Review and recommend modifications to these policies to remain current with changing technology and issues relative to information sharing, confidentiality, and data security.

ISD staff may monitor equipment, systems, and network traffic at any time for security, network maintenance and policy compliance purposes.

The City will conduct assessments on a periodic basis to ensure compliance with this policy.

PRIVACY

With the exception of data and information protected by law, information employees create or use on City systems is not necessarily confidential or private. All of the City's Electronic Media and information relating to these electronic media are City property. Although employees have passwords that restrict access to their computers, the City reserves the right to access this information. While Electronic Media files and information will not be monitored as a routine matter, the City reserves the right to do so without prior notification. By way of example, the City may electronically scan email messages for the presence of specific content such as viruses, malicious code, or passwords, and to maintain system integrity. The City will also respond to legal processes and fulfill any obligations to third parties.

Only Department Heads, Council Appointees or the Information Systems Manager can authorize the reading of Electronic Media information, which includes, but is not limited to, email and voicemail messages, for employees under their supervision. For clarification, Electronic Media related to Lodi City Council Members is managed and supervised the City Clerk.

UNACCEPTABLE USE

The following activities are prohibited; however, any information by the City regarding illegal activities under local, state, federal, or international laws will be turned over to the appropriate authorities. The list below is by no means exhaustive, but attempts to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

- Products that are not appropriately licensed for use by the City or those that violate the rights of any person or organization 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 cannot be used on City equipment.
- 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 the City or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws is illegal. Consult management prior to exporting any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, spyware, etc.) is prohibited.
- Using a City computing asset to actively engage in procuring or transmitting material in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Using a City computing asset to actively engage in procuring, storing, transmitting or viewing sexually graphic material, child-pornography, or sexual material that is in violation of local, state, federal, or international laws.
- Making fraudulent offers of products, items, or services originating from any City account or redirecting or "capturing" intranet or Internet traffic destined for legitimate websites to fraudulent websites.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the individual is not an intended recipient or logging into a server or account that the individual is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Deliberate introduction of monitoring software (a.k.a. "spyware"), remote control software (e.g. WinVNC), or the attachment of devices, whether physically or in close proximity, for the purpose of capturing keystrokes (a.k.a. "key-loggers") onto a computer, without the end-user's permission, is expressly prohibited.

Exception to this would be software or devices provided by law enforcement as part of an official criminal investigations, or ISD for routine purposes.

- Port scanning or security scanning of internal or external networks is expressly prohibited unless these activities are within defined job duties and specifically authorized by the Information Systems Manager, or Network Administrator and the Deputy City Manager/Internal Services Director.
- Executing any form of network monitoring unless defined by job duties and specifically authorized by the Information Systems Manager or Network Administrator and the Deputy City Manager/Internal Services Director.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with or denying service to any user (e.g., denial of service attack).
- 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.
- Providing information about, or lists of, City employees to parties outside the City, or for personal use, without department head and City Attorney approval.
- Establishing remote access to City data networks, computer assets or communication systems without approval of the department head and the City's Information Systems Manager or designated Information Systems Division staff.
- Authorized users are assigned accounts for their specific use based on the defined needs of their position with the City. Users are responsible for the security of their accounts. Passwords are provided to enable users to keep their account secure. Users are not authorized to share their passwords.

WIRELESS NETWORK EQUIPMENT

Written permission must be obtained from the Information Systems Manager or authorized ISD staff before any wireless network device can be connected to internal City networks.

Security settings and personal firewall features must be enabled when using City equipment with wireless capabilities.

Wireless network packet "sniffing" utilities and scanning tools are not allowed to be used in or near City owned buildings or facilities unless authorized by the Information Systems Manager.

ELECTRONIC MAIL (EMAIL) AND MESSAGING

In addition to the foregoing provisions, employees should be aware that certain kinds of Electronic Media may be subject to record retention requirements or disclosure, either as "public records" or pursuant to discovery in litigation.

Email Retention: 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, floppy 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.

Unacceptable Email Use: The following activities are prohibited. Information regarding illegal activities under local, state, federal, or international laws will be turned over to the appropriate authorities. The list below, while not exhaustive, provides a framework for activities that fall into the category of unacceptable email or messaging use.

- Accessing messaging services such as, but not limited to Yahoo Messenger, MSN Messenger or Instant Messaging using City Electronic Media resources without department head authorization is strictly prohibited.
- Sending harassing, threatening, or violent messages is prohibited.
- Forgery of email, including concealment of the sender's identity, is prohibited.
- Sending general or broadcast announcements to all email recipients by individuals is prohibited. Only designated staff are allowed to send broadcast announcements via email, voicemail, or network messaging.
- Creating, storing, sending or forwarding email SPAM (i.e. unsolicited messages that are non-work related), chain letters, solicitations, or advertising, to any internal or external email recipient is prohibited.
- Using a City Electronic Media asset to actively engage in procuring, storing, transmitting viewing, sending, forwarding or relaying sexually graphic material, child-pornography, or sexual images, that is in violation of local, state, federal, or international laws, to any internal or external email recipient or system is prohibited.
- Use of City e-mail account for non-work related purposes.

PORTABLE COMPUTING AND MEDIA

The following minimum requirements for securing all portable computing and media devices (e.g. Personal Digital Assistants (PDA), USB drives, laptop/tablet-PC/hand-held computers, and cellular/wireless telephones) shall be enforced. Due to the prevalence of convenient portable media used in enhancing productivity, the need for organizational controls and oversight are paramount. This policy is designed to ensure that the mobility and ease of use does not lead to inadvertent or accidental

disclosure, loss or misuse of City informational assets. Portable Computing and Media controls shall include the following items:

- City information should only be copied onto portable media when there is a valid business need to do so.
- Any information stored on portable media shall, at a minimum, be secured by password.
- Depending on the type of device, file protection tools should be enabled to protect any information stored on portable media. This may include, but is not limited to encryption, passwords, third party security products, encrypted file systems or other security measures.
- Portable media should be securely stored and safeguarded against theft, loss, or unauthorized access or usage at all times.
- Portable media used to backup information shall be protected from loss or damage and be password protected.
- Portable Media Disposal: Before disposal of portable media, the information stored on these devices should be removed or sanitized.

SECTION 2: NETWORK ACCESS AND ACCEPTABLE USE

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.

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 City-issued network or system User ID's.

General

- Use of the City of Lodi's network shall be in accordance with all applicable rules, regulations, and policies.
- 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.
- 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, Department Head and Deputy City Manager, when circumstances warrant.
- Virtual Private Network (VPN) access shall be granted only upon completion of a properly signed and executed VPN Acceptable Use Agreement and approved by the Information Systems Manager and Department Head.

- IBM user accounts shall be issued only upon completion of a properly signed and executed User Access Application.

Access to City of Lodi's Network

- 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.
- 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.

NETWORK ACCOUNTS AND PASSWORDS

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.

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).

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/her designee, or the Network Administrator.

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:

- 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.
- Department Heads 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.
- 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.
- Department Heads are responsible for approving access requests to shared directories for City of Lodi’s users outside of the defined work unit. Department Heads shall forward approved requests to the ISD Help Desk for implementation.
- The Information Systems Division shall determine the location of applications files. Installation of software is the responsibility of ISD.

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.

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

Acceptable Usage Policy. Inappropriate use will be subject to loss of account privileges or disciplinary action, up to and including dismissal.

Personal Home Directory:

- Only the named user will have rights to that user's personal home directory.
- 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.).
- Designated ISD technical staff may obtain access when necessary in their duty of supporting the user of the account.

Shared Directory:

- Only those users or groups of users determined by specific departments or divisions shall have rights to designated shared directories.
- 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.).
- Designated City of Lodi technical staff may obtain access when necessary in their duty of supporting the user of the account.

Local Hard Drive:

- The user of the desktop has access to the local drive. This drive is not necessarily secure from access by unauthorized users.
- 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.
- ISD does not perform routine backups of the hard drive contents.
- Designated ISD technical staff may obtain access when necessary in their duty of supporting the user of the account.

Prohibitions

- Sending or sharing with unauthorized persons any information that is confidential by federal or state law, rule or regulation or City policy.
- Installing software that has not been authorized by the respective department head in concurrence with the Information Systems Division
- 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

- Attaching processing devices that have not been authorized by the respective department head in concurrence with the Information Systems Division
- Using network resources to play or download games, music or videos that are not in support of business functions
- Leaving workstation unattended without engaging password protection for the keyboard or workstation
- Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing
- Using network resources in support of unlawful activities as defined by federal, state, and local law
- Utilizing network resources for activities that violate policies established by the City of Lodi.
- City network resources may not be used to engage in union or bargaining unit activities
- Users shall not share their passwords and shall be solely responsible for maintaining the secrecy of their password.

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.

- 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.
- Users shall be limited to the following storage limits: 50MB for email, 75MB for network files.

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.

- Network backups will include all network directories, including all personal and shared folders.
- 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 only short periods of time.
- 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.

Local Hard Drive Backup

- 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.

Periodic reviews of users and user rights

- The 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 the Information Systems Division any changes in users or their respective access rights, and the Information Systems Division personnel shall adjust in a timely manner the users and user rights as recommended by the department heads. The reviewed lists of system and application users shall be kept on file by the Information Systems Division as documentation of these actions.

SECTION 3: SOCIAL NETWORKING

PURPOSE

The purpose of this policy is to reduce the City's security risks; protect the productivity of its employees; reduce the reputational risk to employees, Departments and the City; mitigate the potential risk of exposure or leakage of sensitive or protected information such as copyrighted material, intellectual property, personally identifying information, etc.; to manage network bandwidth; and to reduce the potential for malware introduction into the City's Information Technology environment.

For the purpose of this policy, "social networking" is defined as interactive communication in which participants in online communities share thoughts via text, photographs, video, audio, etc. Online communities or "social media" include, but are not limited to, Facebook, MySpace, YouTube, Twitter and similar websites.

SCOPE

This policy shall apply to all City departments and staff. Individual departments may adopt Social Networking policies for their staff that are more restrictive than this policy, but may not adopt policies that are more permissive than this policy.

POLICY

IT Administrator Requirements: The City's Information Systems Division (ISD) shall limit Internet access to Social Media web sites according to the limitations of the City's Electronic Media Acceptable Usage and Web Filtering Policies. All users, except elected officials, shall be blocked, by default, from

Social Media sites. Exceptions shall be based upon the terms and conditions set forth in the City's current Web Filtering Policy.

User Requirements:

- Users shall connect to, and exchange information with, only those Social Media web sites that have been authorized by the appropriate Department Head in accordance with the requirements within this and other City policies.

- Users shall minimize their use of "other than government" sections of the Social Media web sites.

- Users shall not post or release proprietary, confidential, sensitive, personally identifiable information, or other City government Intellectual Property on Social Media web sites.

- Users who connect to Social Media web sites through City computing assets, who speak officially on behalf of the City, or who may be perceived as speaking on behalf of the City, are subject to City requirements addressing prohibited or inappropriate behavior in the workplace, including acceptable use policies, user agreements, sexual harassment policies, etc.

- Users shall not speak in Social Media web sites or other on-line forums on behalf of the City, unless specifically authorized by the user's Department Head or the City Manager.

- Users who are authorized to speak on behalf of the City of Lodi shall identify themselves by: 1) Full Name; 2) Title; 3) Department; and 4) Contact Information, when posting or exchanging information on Social Media forums, and shall address issues only within the scope of their specific authorization.

- Users who are not authorized to speak on behalf of the City of Lodi shall clarify that the information is being presented on the user's personal behalf and does not represent any position or policy of the City.

- Users shall not utilize tools or techniques to spoof, masquerade, or assume any identity or credentials except for legitimate law enforcement purposes, or for other legitimate City purposes as defined in this or other City policies.

- Users shall avoid mixing their professional information with their personal information.

- Users shall not use their work password on Social Media web sites.

SECTION 4: WEB FILTERING

PURPOSE
The purpose of this policy is to reduce the City's security risks, protect the productivity of its employees, and to manage network bandwidth via controlled access to Internet Web sites.

SCOPE
This policy shall apply to all City departments and employees with access to the Internet from City networks.

POLICY
Web Filtering Technology: All Internet access through City networks shall be subject to Web filtering technology. Department Heads will ensure that web access is used only for required departmental business functions.

Web Filtering: Anyone accessing the Internet through City networks will be governed by rules implemented through web filtering. Rules will be established by the City's Information Systems Division (ISD), subject to the approval of the City Manager. Exceptions to current Web filtering rules may be granted to individuals upon request and upon approval of the appropriate Department Head. Incidental exceptions may be granted at ISD's discretion. Written documentation identifying each exception will be maintained by ISD.

Web Filtering Selection: Blocked sites shall be based on a list developed and maintained by ISD, or an independent subscription service, subject to approval by the City Manager. Such sites shall be identified by either category or domain. The City may subscribe to an independent service that will categorize all Internet sites and URLs. Sites or categories on this list may be blocked for all City users, at the City's discretion. Exceptions may be made, as referenced in this Policy.
Exceptions to the established Web Filtering rules must meet the following criteria:

- Must be for legitimate departmental business purposes.
- Must not expose the City or its computing or network infrastructure to excessive risk or bandwidth reduction, as determined by ISD.
- Must be for a determinate period, e.g. one day, one month, or one year. Exceptions must be re-evaluated by ISD every six months. Exceptions may be renewed for up to one year. Departments must notify ISD in a timely fashion, in writing (email), when an exception is no longer justified under this Policy.
- Individuals who have been granted an exception to the established Web Filtering rules may be required to log in for authentication purposes. Sharing one's login credentials for the purpose of circumventing this Policy, or any other reason, is against City policy and strictly forbidden.

SECTION 5: SOFTWARE SELECTION AND ACQUISITION

PURPOSE

As information systems are replaced and new ones put into place, it is in the best interests of the City to establish a process and procedure for selecting and acquiring software in order to ensure that needs are met while the greatest value is realized. The purpose of this Policy is to formalize the process for selecting and obtaining the most suitable software in a timely manner, at the lowest cost, and which will meet user needs in conjunction with and as further clarification to the policies and procedures contained in the City's Purchasing Policy.

General. Three categories of software have been identified. The following process and procedure does not apply to personal applications as described below.

Enterprise Systems and Applications: Software that uses a database as its "backend" and is multi-user within a department or has users in multiple departments.

Limited Use Applications: Software used for specialized applications within a Department or division

Personal Applications: Software used or developed by one employee

Although these definitions have been designed to address the varying needs during the acquisition of these types of software, it is recognized that not all software purchases will fit neatly into one of these categories. The degree of integration with the City's existing computing environment will greatly influence who should be involved in the software selection and acquisition process.

Procedure for new, upgrade or expansion of existing software

The following steps are established for software acquisitions and pertain primarily when the acquisition involves an expenditure of $20,000 or more, are for Enterprise Systems or Applications as herein defined, or affect a user group larger than 25. They may be reduced or eliminated for Limited Use Applications or less comprehensive acquisitions, with concurrence of the Information Systems Manager and the City Manager.

Recognize Need, Appoint Committee and/or Project Manager: For Enterprise Systems and Applications, a project committee shall be appointed with the majority of members being users from functional areas and end users, joined by information systems staff, whose chairman is jointly selected by the Information Systems Manager and the City Manager's Office. The role of the Committee shall be to represent all of the departments, divisions and users who will be affected by the Project, in addition to overseeing the successful completion of the following steps. A Project Manager may be appointed by the Information Systems Manager and affected Department heads in lieu of a Committee.

Procurement Process: In all cases, the City's established Purchasing Policy guidelines shall apply.

Define General Needs and Develop Budget Projection: General needs should be identified based on the problems to be solved as well as what could reasonably be expected to be available in the marketplace. Preliminary budget projections may cover only the cost of software and a general estimate of other expenses.

Investigate the Market: Investigating the market may involve site visits, communication with other institutions using the product, vendor demonstrations, or a Request for Information (RFI). A Business Case Analysis or Cost Benefit Analysis shall be completed as part of this investigation, including a section describing Total Cost of Ownership (TCO) and Return On Investment (ROI).

Refine the Budget and Identify a Funding Plan: Before proceeding with the project, a refined budget plan should be prepared which covers all costs of consulting, acquisition, licensing, hardware, additional staffing, implementation, testing, training, maintenance, and upgrades, for a five year period. Consideration should also be given to costs of integration with existing systems, and to savings which may be obtained from phasing out systems that are no longer needed. Identify funding sources and obtain appropriate approvals.

Define Detailed Needs: A thorough needs analysis of software requirements should be conducted. For example, for a Human Resources system, this analysis should encompass the needs of functional staff (such as Human Resources), end users (such as departmental users), and technical staff (such as ISD staff responsible for maintaining the system). The analysis should distinguish between required and desired capabilities and should also cover such things as maintenance, support, training, upgrades, existing or proposed hardware, and the computing infrastructure. If necessary, the budget plan should be revised.

Upon completion of the needs analysis, if it is determined that a critical, mandatory feature is only available from one vendor, and only from one distribution source, a designated committee representative should develop the justification for a sole source purchase. If appropriate justification is provided, it will not be necessary to issue an RFP. Upon approval of the sole source justification by the City Manager, a written offering should be sought from the sole source vendor and evaluated for its fulfillment of the identified needs.

Purchasing Procedure: "Acquisition of electronic hardware and software shall be by negotiation, requests for proposal, or competitive bids, and award shall be based on 'best value' criteria as established by [Lodi Municipal Code] Section 3.20.015, under direction of the information systems manager, and

set forth in the terms of the negotiation, request for proposals, or bid. Alternatively, purchase of electronic hardware and software may be made in accordance with [Lodi Municipal Code] Section 3.20.045. (Ord. 1763 § 2 (part), 2005). The bidding process described in this code may be waived when advantageous for the city, and authorized by the city manager for purchase of supplies, equipment or contractual services awarded in accordance with formally adopted bidding or negotiation procedures approved by the governing boards of other California public agencies. Purchases or contracts in excess of twenty thousand dollars shall require the approval of the city council. (Ord. 1763 § 2 (part), 2005)"

Follow Purchasing Policy software purchasing guidelines (see City's current Purchasing Policy as set forth in the Lodi Municipal Code.)

Follow Change Control Policy for implementation procedures (see City's Change Control Policy set forth below).

Maintenance

The initial periods of maintenance should be included in the RFP specifications.

SECTION 6: CHANGE CONTROL

PURPOSE

As information systems are modified or replaced and as new systems are put into place, the changes may impact the confidentiality, integrity or availability of information in the system. To reduce the likelihood of such unanticipated consequences, this Policy establishes a mandatory "change control" process whereby changes to Enterprise Systems or Applications and departmentally supported systems shall be documented as herein set forth.

POLICY

Change control is good practice for any system. The change control requirement instituted by this Policy applies to any Enterprise System or Application or departmentally supported system of the City. For the purposes of this Policy, an Enterprise System or Application is one that uses a database as its "backend" and is used by more than just one person (i.e. is not considered a personal application). Departmentally supported systems are those systems and applications that are supported at the department level with little or no support provided by the Information Systems Division.

This Policy, which applies to all employees identified by the Information Systems Division (ISD) as being authorized to modify, patch or make changes to City systems, shall implement a change control process for such systems in order to minimize the possibility of security risks and access disruption that can be caused by inadequately tested or implemented changes. Changes to any system or application shall be tested, documented and authorized, as deemed appropriate by the Information Systems Manager, or designee, for ISD supported systems. For

departmentally supported systems, change requests shall be tested, documented and authorized by the appropriate Department Head and ISD. ISD shall acknowledge the change request by email, telephone or other appropriate means within two working days of receiving the request. The person responsible for creating the change shall not also authorize the move into the production environment. Instead, the Information Systems Manager or designee (or Department Head for departmentally supported systems) shall authorize the move to production.

1) Procedure

   a) Change Request: Users shall submit requested changes to their appropriate supervisor for approval. Following approval by the appropriate Department Head, requests shall be forwarded to Information Systems Division personnel via the Helpdesk Request system. ISD shall acknowledge the change request within two working days of receiving the request. Change requests shall specify reasons for the change and describe the nature of the requested change. A business case justification may be required at the discretion of the Information Systems Manager or the affected Department Head for departmentally supported systems. In cases where changes are initiated by ISD staff, the staff person shall notify the Information Systems Manager, or designee, of the change request and log such request through the Helpdesk system.

   b) Information Risk Assessment: ISD staff assigned to the change request shall conduct a risk assessment to identify threats and vulnerabilities that result from the requested change to a process or a system, as needed. The Information Services Manager, or designee, will work with department staff on the risk assessment for departmentally supported systems. The risk review and recommendations for addressing any identified risks shall be documented, and said documentation shall be retained by ISD for a period of one year after change is implemented. The Information Systems Manager or Network Administrator, or designees, shall be consulted on risks whenever new systems or upgrades are planned.

   c) Approvals Major Upgrades: All changes and upgrades to systems or applications shall first be approved by the Information Systems Manager, applicable Department Head(s) and the City Manager's office.

   d) Documentation: All system and configuration changes shall be documented in a change control log (example and required format attached). Documentation shall include details about what was changed or modified, how changes were made, name and location of relative files or objects, issues or problems encountered while implementing the change and what the resolutions were, and contact information for outside vendors or personnel who assisted with the project. All documentation referenced in this policy shall be filed with the Information Systems Manager, or his designee. Documentation of program changes inside the

program do not replace the need for documentation in the change control log.

e) Backup: A backup of all system software, system configurations, applications and data installed on systems shall take place prior to deployment of a changed or upgraded system. The backup process provides a method to restore systems if the change process fails.

f) Training: As far as possible and as part of deployment for new or significantly modified systems, both ISD and affected users shall be adequately trained on the new, changed or upgraded systems.

g) Testing: As required by the Information Systems Manager, or designee, a user shall test all changes prior to their deployment on a production system. An individual or entity other than the developer of the new or updated system shall perform the test. The testing shall include verification that all expected functionality exists and performs as needed. To the extent possible, testing should include positive testing to validate expected results and negative testing to ensure no unanticipated impacts occur. The results from testing shall be documented, including how tests were done, what files or objects were included in the test, and what problems were encountered, if any, along with a description of solutions to problems encountered. Such testing results shall be retained by ISD until the system is no longer used in production. Program testing must be reviewed and approved by the Information Systems Manager, or designee, before implementation into the production environment. For departmentally supported systems, the Information Systems Manager and the appropriate Department Head shall review and approve testing before implementation into the production environment.

h) Move to Production: The process of moving new or modified programs into the production system shall be performed by someone other than the programmer who developed it or managed the project.

i) Customer Notification: Affected users shall be notified at least seven business days prior to the production implementation of any new or modified system or program. Notification may be done via email, telephone, or other suitable means of communication. If the modification will have no meaningful impact on users, then notification may be limited to the respective department or division head. In all cases the Information Systems Manager shall be notified before any new or modified system or program is put into production.

SECTION 7: PATCH MANAGEMENT

PURPOSE

The purpose of this Policy is to ensure computer systems attached to the City of Lodi network are updated accurately and in a timely fashion with security protection

mechanisms (patches) for known vulnerabilities and exploits, and for fixing or improving the underlying software. These mechanisms are intended to reduce or eliminate the vulnerabilities, exploits and problems with limited impact to the business.

POLICY

This policy applies to all employees identified by the Internal Services Division as being authorized to apply patches as herein described. City of Lodi computing resources have been developed to encourage widespread access and distribution of data and information for the purpose of accomplishing the missions of the organization.

General

- Patch management for operating systems and applications shall follow current Change Control policy and procedures.
- All networked devices belonging to or managed by City of Lodi departments, divisions, or other affiliated or partner organizations, will be patched with vendor provided updates, patches and fixes.
- All updates, regardless of their type (whether they are service packs, hotfixes or security patches), are to be applied according to their criticality as determined by the Information Systems Manager, Network Administrator, or their designee(s).
- Once alerted to a new patch, Information Systems Division, or departmental, personnel will download and review the new patch within 24 hours of its availability, or as soon as possible after download. Information Systems Division personnel shall categorize the criticality of the patch according to the following:

  Emergency — an imminent threat to City of Lodi network

  Critical — targets a security vulnerability

  Not Critical — a standard patch release update

Before applying any service pack, hotfix or security patch, all relevant documentation will be read and, depending upon its criticality as determined by the Information Systems Manager, Network Administrator, or their designee, peer reviewed as a way of mitigating the risk of a single person missing critical and relevant points when evaluating the update.

To the extent possible or practical, service packs and hotfixes must be tested on a representative non-production environment prior to being deployed to production.

Where possible, service packs, hotfixes and security patches must be installed such that they can be uninstalled, if required. If the patch does not allow for it to be uninstalled then a back-out plan must be developed prior to

the application of the patch that will allow the system and enterprise to return to their original state.

A full system backup should be done just prior to implementing patches, hotfixes or service packs to production systems so that restoration to original state can be completed, if necessary.

Helpdesk staff and unit managers should be notified of the pending changes so they may be ready for arising issues or outages. Notifications shall be made via email or other appropriate communications method, as determined by the Information Systems Manager or designee, in compliance with the seven day notice procedure as described in the Change Control Policy, or at least 24 hours in advance of scheduled patch application.

SECTION 8: E-WASTE DISPOSAL

PURPOSE

The purpose of this Policy is to set forth procedures and guidelines for the appropriate and responsible disposal of retired or surplus electronic components, also known as "e-waste." This Policy applies to all departments and employees of the City.

INCLUDED COMPONENTS

Electronic components subject to this Policy are included on, but not limited to, the following list:

Computers (CPU) (includes desktop, laptop, server)
External data storage/back-up devices
PDAs and "smart phones"
Copiers that have data storage capability
Printers (includes all types, laser, inkjet, bubble jet, dot matrix, plotters, etc.)
Telephone systems and handsets, cellular Phones, cell phone batteries, cell phone headsets
Hubs, routers, switches
Peripherals (includes keyboards, mouse, speakers, monitors)
Fax machines

POLICY

Before transferring or disposing of surplus electronic equipment, special procedures must be followed to protect data confidentiality and to ensure compliance with federal copyright laws, software licensing agreements and waste disposal regulations.

All computer systems and electronic devices shall be properly cleaned of sensitive data and software by the removal of hard drives and RAM memory before being

disposed of, recycled, returned to vendors, sold or otherwise transferred outside the City.

Hard drives must be sanitized by using software that is compliant with Department of Defense standards, or physically destroyed. Non-rewritable media, such as CDs or non-usable hard drives, must be physically destroyed.

Memory sticks or modules, including flash memory, must be destroyed if they are not to be re-used by the City.

Information Systems Division (ISD) has primary responsibility for deeming that an electronic component included in this Policy is to be retired, receiving removed storage devices and memory modules, and for their destruction or cleaning.

Computer and other electronic equipment referred to in this Policy may be deemed surplus by ISD personnel, using the following criteria:

1. IT equipment that no longer supports software used by the City
2. Is not interoperable with other required IT equipment
3. Is not cost effective to make interoperable with other required IT equipment used by the City
4. Component is non-functional and cannot be repaired, or cannot be made suitably functional by upgrading or replacing parts

PROCEDURE

The following procedure will be followed for surplus or retired equipment:

i) Notification: Departments shall notify ISD through the Helpdesk system when a piece of electronic equipment referred to in this Policy is suspected of needing to be replaced or retired.

ii) Assessment. ISD shall make an assessment of the component's condition and determine the best course of action, whether it can be repaired or upgraded, or should be retired.

iii) Device Removal: ISD personnel, or their designee, shall remove hard drives and memory devices, as herein described, from systems and components deemed to be retired.

iv) Remove ID Tags: City asset ID tags shall be removed from systems and components before disposal, sale or recycling.

v) Device Cleansing or Destruction: ISD shall, at its discretion, cleanse memory and storage devices if they are to be reused, or destroy, or cause to be destroyed, if they are going to be disposed of. A certificate of destruction shall be secured if a third party is hired to perform the destruction and disposal of these components.

vi) Update Inventory: An inventory listing of all computers, including details of each unit, and network devices and components shall be kept by ISD. Electronic equipment covered by this Policy that is retired or is transferred from the City shall be removed from inventory by notation.

(1) ISD shall notify Finance of items removed from its inventory so that the fixed asset records can be updated.

vii) Transported for Disposal: Retired electronic equipment covered under this Policy shall be transported to the city's warehouse for final disposition.

(1) Equipment for disposal shall bear a stamp or mark from ISD indicating that it has been cleansed of confidential data and is ready for disposal.

viii) Disposal: Electronic equipment covered by this Policy may be sold, donated, recycled or destroyed according to applicable city policy at the discretion of the City Manager or Internal Services Department director.

ix) Recycling: All applicable laws governing the disposal or recycling of electronic equipment, parts and components must be followed. Vendors must provide the City with certification that all components were recycled in accordance with applicable federal, state and local laws and regulations governing such activities.

x) Cost of disposal: Costs associated with disposal of e-waste, if any, shall be borne by the Purchasing Division of the Internal Services Department.