



Technology Policies

2003

Table of Contents

Adopted January 14, 2002

GENERAL SECTIONS.....	3
PURPOSE.....	3
BACKGROUND	3
DEFINITIONS.....	3
SCOPE.....	3
SYSTEM OWNERSHIP	4
SYSTEM INSPECTION OR REVIEW.....	4
GENERAL POLICIES	4
LIMITED PERSONAL USE POLICY.....	5
RESPONSIBILITIES.....	6
REVIEW PROCEDURES	7
ENFORCEMENT	7
COMPUTER POLICY	7
GENERAL.....	7
UNIFORMITY.....	7
HARDWARE PURCHASES.....	8
E-MAIL/ INTERNET ACCESS POLICY.....	9
DEFINITIONS.....	9
POLICY.....	9
E-MAIL RETENTION POLICY.....	10
ACCESS TO NETWORK/HOST COMPUTERS POLICY	11
DEFINITIONS.....	11
SCOPE.....	11
POLICY.....	11
SOFTWARE POLICY.....	12
DEFINITIONS.....	12
SCOPE.....	12
POLICY.....	12
PASSWORD SECURITY POLICY	12
POLICY.....	12
PRINTERS POLICY.....	13
DEFINITIONS.....	13
POLICY.....	13

ADDENDUM A: PERMITTED SOFTWARE

Electronic Equipment Systems Policies

GENERAL SECTIONS

Purpose

To establish policies for the proper use of electronic equipment systems provided by the City of Belmont (the “City”) to its employees in the performance of job related functions and/or assignments. The various components of this policy are intended to allow the City to derive the benefits of increased efficiency through the use of electronic equipment while insuring the protection of information assets, City integrity, and employee rights. The beginning sections of the policy are general and refer to all aspects of the City’s electronic equipment systems. The later sections are more detailed and specific to individual components of the System.

Background

Computers and other electronic systems have become an indispensable business tool, easing communications, enhancing work flow, increasing productivity and performing a variety of other business functions. They have provided a foundation for fostering and improving employee communications; they have allowed us to reduce our general expenses by increasing efficiency and decreasing the need for paper and other products. The City encourages the business use of electronic equipment systems for all employees. This is intended to create a formal policy regarding the appropriate use of such systems and to inform employees and managers of their rights and responsibilities associated with their use.

Definitions

1. The term “Electronic Equipment System: (the “System”), shall mean all computers, hardware, software, and tools owned, leased, rented or licensed by the City which is made available for official use by City employees (“Employees”).
2. The term “Tools” shall include, but is not limited to, electronic mail (“e-mail”), the Internet, and such other similar software or applications available on the System.
3. The term “Hardware” shall include, but is not limited to computer terminals, network equipment, modems or any other tangible computer device generally understood to comprise hardware.
4. The term “Software” shall include, but is not limited to all computer programs, other than the Tools available on the System.
5. The term “Temporary or Permanent File” shall mean any electronic document, information or data residing or located, in whole or in part, on the System, including but not limited to spreadsheets, calendar entries, appointments, tasks or notes.

Scope

This policy applies to:

- a. All City employees including permanent, temporary, part-time and contract employees, and to all other users of any City electronic equipment system regardless of their affiliation.

b. All City owned or operated electronic equipment system, or systems which are subscribed to and paid for by the City.

c. All electronically-generated data.

System Ownership

The System, any and all Temporary or Permanent Files, and related electronic systems or devices are, and shall remain the sole property of the City.

System Inspection or Review

Employees do not have a right, nor should they have an expectation, of privacy while using any City System. By using the City's System, employees imply their consent to disclosing the contents of any files or information maintained or passed-through the City's System.

By using the System, consent to monitoring and recording is implied. Any use of City resources is done so with the understanding that such use is generally not secure, is not private, and is not anonymous.

The Information System Manager (IS Manager) does employ monitoring tools to detect improper use.

Electronic communications may be disclosed to supervisors who have a demonstrated need to know in the performance of their duties.

An Employee's supervisor has the express authority to inspect or review the System, any and all Temporary or Permanent Files, and related electronic systems or devices and any contents thereof so long as such inspection or review is in the ordinary course of their supervisory duties.

Reasons for inspection or review may include, but are not limited to System malfunctions, problems or general System failure, a law suit against the City involving the Employee or related to the Employee's duties, violation of a City policy, or a need to perform or provide a service when the employee is unavailable.

When requested by an Employee's supervisor, or during the course of regular duties requiring such information, a member(s) of the Information Services staff may extract, download, or otherwise obtain any and all Temporary or Permanent Files residing or located in or on the System.

General Policies

- Information received into the City's System or created in the City's System is presumed to be a public record unless the document falls within an exemption pursuant to the applicable provisions of the California Government Code.

- Because the information contained in the City's system is presumed to be a public record, it shall only be deleted from the System in compliance with the City's records retention/destruction policy.
- All Employees have a responsibility to protect the System and City property from physical and environmental damage and are also responsible for the correct use, operation, care and maintenance of the System.
- All Employees shall use the City approved virus scan on all diskettes, files, documents or other device which are obtained from a source outside the City or from any non-city computer system.
- It is expressly prohibited for an Employee to allow an unauthorized user to access the System at any time or for any reason.
- Employees shall report any unauthorized access to the System, or suspected intrusion from outside sources via the Internet to their Department Head, supervisor or the IS Manager.
- The City's logo or any other official City symbols may be used on official documents and presentations only.
- The City will create standard forms and formats for use in creating documents.

Limited Personal Use Policy

Generally, employees may use City Systems for authorized purposes only. Taxpayers have the right to depend on the City to manage government resources effectively. Public confidence in the productiveness of government is increased when the public knows the City is well managed and assets are used appropriately. Consequently, employees are expected to follow rules and regulations and to be responsible for their own personal and professional conduct.

Belmont encourages a professionally supportive work environment. Employees are given the tools needed to effectively carry out their assigned responsibilities. Allowing limited personal use of City Systems helps enhance the quality of the workplace and helps retain qualified workers.

Employees are allowed limited personal use of City Systems, as long as this use does not result in loss of employee productivity, interfere with official duties, or have more than a nominal expense to the City. Any personal use should take place during non-work time. The IS Manager shall revoke or limit this privilege upon the direction of the Department Heads or City Manager if it is demonstrated that the employee has violated this policy.

Privilege, in the context of this policy means the City is extending the opportunity to its employees to use government property for personal use in a effort to create a more supportive work environment. However, this policy does not create a right to use City equipment for non-City purposes. Nor does the privilege extend to modifying such equipment, such as loading unauthorized software or making configuration changes.

Nominal expense means the employees personal use of the System is limited to those situations where the City is already providing equipment and the employees use of such equipment will not result in any additional expense to the City beyond normal wear and tear, or the use of small amounts of electricity, ink, toner or paper. Examples of nominal cost include, but are not limited to, making a few photocopies or infrequently sending personal e-mail messages.

Non-work time is defined as time other than during normal business hours. This would include before or after work and at lunch, as long as use of the system is not visible to the public.

Inappropriate use

Employees are expected to conduct themselves professionally in the workplace and to refrain from using City Systems for activities that are inappropriate. Employees are specifically prohibited from using City Systems to maintain or support personal private business. Other examples of inappropriate use include, but are not limited to:

- Use that could cause congestion, delay or disruption of service to City Systems.
- Use for activities that are illegal or offensive to other employees or the public, such as hate speech or sexually-oriented material.
- Use for posting information to external newsgroups, bulletin boards or other public forums without authority.
- Use that could give the false impression that an employee is acting in an official capacity when using City Systems for non-business purposes.

Employees should inform management of any abuses of this policy.

Responsibilities

a. Under this policy, the City is responsible for:

- 1) Informing all new employees about the City's computer policy and insuring that they understand their rights and responsibilities with regard to the use of Systems under this policy. The City Manager or his/her designee will be responsible for disseminating this information.
- 2) Training employees charged with the operation, security and maintenance of City Systems and associated hardware and software in how to discharge their function properly without violating any of the provisions herein. All Divisions/Offices performing security training are responsible for this function.
- 3) Keeping abreast of changes in litigation which may create a need for the revision of this policy, and making the appropriate changes if and when necessitated by these changes. The City Attorney's office is responsible for performing this function.
- 4) Adhering to its MOU's, other fiduciary responsibility regarding Privacy Act Information, employee work rights and any other articles of non-disclosure which are deemed applicable.

b. Under this policy, users of any City provided Systems are responsible for:

- 1) Reading and understanding this policy and its provisions, and making sure that they abide by them.
- 2) Understanding that the City will not be liable for any disclosure of personal information in the event that the employee chooses to send such information.
- 3) Knowing how to classify information which should not be sent through computers due to its sensitivity, or which should be sent through the computer only after it is encrypted.
- 4) Respecting the rights of other employees provided under this policy.

Review Procedures

The City Manager's office and the Technology Steering Committee, in conjunction with the City Attorney, will review and modify this policy and related procedures on a periodic basis and recommend modifications when appropriate.

Enforcement

A copy of this policy will be provided to all employees using or having access to the System. Each employee shall be required to acknowledge in writing that they have received, read and understand the contents of this policy and the consequence of any violation thereof. A signed copy of this acknowledgement shall be given to the employee and a signed copy shall be retained for the employee's personnel file. Violation of this policy or any provision thereof, will be reviewed by the employee's Department Head in consultation with the Information Systems Manager on a case-by-case basis. Violations may result in *loss or limitation of personal use and/or* disciplinary action, up to and including termination, depending on the severity.

<h2>Computer Policy</h2>

1. General

- A. All computers, networking capabilities, software, printers, modems and other accessories are provided by the City of Belmont for use by its employees and agents as a tool to assist them in performing assigned job duties.
- B. All documents, software, programs/macros written are the property of the City when City resources are used to create and/or purchase them.

2. Uniformity

- A. It is desirable to create standards where appropriate across all computer platforms. The intent is to enhance the use of the enterprise for City staff and not to overburden them with different procedures and policies for different systems.
- B. Strict security enforcement and adherence to established login and password protocol will be implemented across the enterprise to minimize potential security breaches. Changes in

passwords can be done with the notification of the IS staff. If IS staff changes a password, the user will be notified.

- C. Standards put in place to ease the use of the enterprise should not jeopardize the security or integrity of any individual system or department need. System-wide standards should respect the inherent differences between operating systems and platforms.

3. Hardware Purchases

- A. Purchasing New Equipment: The purchase of new computer equipment must be approved through the Technology Department, budget process and have adequate written justification or be part of the electronic equipment purchase and replacement schedule. Proposed purchases must comply with the goals and objectives of the City's Technology Plan.

1. Personal Digital Assistants (PDAs)

With the growing need for instantaneous communication and data access, the City has seen a significant increase in the use of the Personal Digital Assistant (PDA) devices. This section is intended to provide guidance to departments or individuals who are utilizing PDAs or considering implementing the use of them in their daily work.

The PDA is not considered a secure computing device. It is recommended that only non-confidential information be stored on the device and the password protection feature enabled.

PDAs must meet the City's hardware and software standards in order to receive support for the device.

The I.S. Manager will administer the PDA Support Policy and the I.S. Division will provide limited technical assistance for supported PDAs as resources permit. The City will not be responsible for providing the PDA, except in limited situations.

- B. Repair/Replacement of Existing Equipment: The City has generally implemented a 3 year replacement schedule for personal computers. Some computers may need to be replaced before the end of 3 years based on repair and maintenance for each computer. Some computers may also continue to be used longer than the expected 3 year lifespan.
- C. Disposing of Outdated Equipment: If the City determines that a piece of electronic equipment is "excess." The hard drive of the computer or any other media used in the computer for data storage will be erased using software that permanently removes City data from the computer. Staff should notify IS if they believe a piece of electronic equipment is surplus.

E-Mail/ Internet Access Policy

1. Definitions.

The following definitions apply through this policy:

- a. E-Mail. Electronic mail. Automated system for sending and receiving electronic message through a computerized network.
- b. The Internet. Medium of communication based upon the integration of land area networks.
- c. Business Day Related Communication. Any communication which occurs during the normal accomplishment of ones duties or job function. For example, it is acceptable to send a mail message to a colleague to set up a lunch appointment, but not to sell football tickets. The City has an electronic bulletin board on the shared drive for employees to use for non-business related communication.

2. Policy.

- A. The use of e-mail to harass or annoy other City Employees is explicitly and expressly prohibited at all times.
- B. Use of e-mail and the Internet must not interfere with work as established in job functions and duties assigned.
- C. All Employees using or accessing the Internet hereby acknowledge the serious nature and existence of computer viruses. Employees shall be conscientious and remain vigilant in protecting the safety and security of the System. No Employee shall download files or information from the Internet without first scanning those files using the proper virus scanning program to protect the System from potential risk of or infection from such a virus. No software programs shall be downloaded until prior authorization from an Information Services employee.
- D. Because there are security issues with allowing access to City systems through the Internet, the City reserves the right to monitor all employee e-mail, and Internet transactions.
- E. Response Expectations to e-mail: City staff is expected to respond to e-mail requests within one business day, unless there are mitigating circumstances to prevent access to these forms of communication. (i.e. vacation, illness, conference attendance, etc.) E-mail should not be used to replace *all* written communication but rather to augment it.

If an employee fails to respond to an e-mail message, it shall be given the same weight as failure to respond to a written communication. The exception to this is failure to respond when it is shown that the e-mail message was not received due to system failure.
- F. Because of security risks, confidential information should NOT be conveyed by e-mail.

E-MAIL RETENTION POLICY

Electronic mail may be covered by public records laws and users of electronic mail (e-mail) should be aware of retention issues.

E-mail is not intended for permanent storage on the PC. Users should not hold e-mail messages in their system for more than 60 days. After 60 days, messages are to be deleted by the user from their "Inbox" as well as their "Deleted Items" folder.

All e-mail messages are held for 30 days on tape backup by the Information Services Division but City backups of the e-mail system are not sufficient for the various record retention requirements (see your department's copy of the City's records retention schedule).

In the event information in an e-mail message relates to a current project/policy-making decision, or otherwise needs to be retained, the message should be printed and placed in the proper hard-copy file or transferred electronically to the administrative record of an online project file.

Process for deletion in user's mailbox:

1. In folder list, right click on Deleted Items.
2. Choose "Empty Deleted Items Folder".

Process if you would like to set up your system so it automatically deletes email after 60 days:

1. Right click Inbox or whichever folder(s) you have email come in to.
2. Left click on Properties
3. Left click on AutoArchive Tab
4. Check box "Clean out items older than 2 months.
5. Un "dot" Move old items to
6. "Dot" Permanently delete old items

Process for electronic transfer:

1. Open e-mail message to transfer.
2. Click file, save as, name the file and choose network drive and directory of the pertinent project. (*The e-mail will be saved in .txt (text) format.)

Access to Network/Host Computers Policy

1. Definitions.

The following definitions apply through this policy:

- a. Network. Integrated computer system which allows users from various workstations to communicate with a central mainframe and share data amongst each other.
- b. Server. A central hub computer which stores the shared files of a network.

2. Scope.

This policy applies to: All network data.

3. Policy.

- A. The I.S. Manager and/or designee serves as System Administrator or backup System Administrator for each Network File Server, Workgroup Server or Host Computer. System Administrator responsibilities include assigning new user ID's, establishing user rights, protecting security, maintaining access, privacy, work ethics/standards, removing logins for separating employees, and security of network when personnel issues arise.
- B. Some employees need remote (dial-up) access to City systems. Access will be allowed for just cause and with appropriate security in place. Staff requests for remote access must be submitted in writing to the City Manager or his/her designee for consideration because allowing remote access can be a security risk. Requests for remote access will be reviewed on an individual basis. All security requirements listed above will be enforced for remote access users.
- C. File Storage on PC's/Network/Host Computers:
 - a. The Systems Administrator and Department Heads reserve the right to access and review all data stored on computers owned by the City.
 - b. Data stored on PC's and not on the Citywide Network or a host computer, will not be backed-up on a regular basis. All critical information **MUST** be stored on the Citywide Network or a Host Computer.
 - c. Because PC's are not secure devices, all confidential information must be stored on the Citywide Network or a Host Computer with appropriate security.

Software Policy

1. Definitions.

The following definitions apply through this policy:

- a. Software. Software is a general term for the various kinds of programs used to operate computers and related devices.
- b. Business Related Communication. Any communication which occurs during the normal accomplishment of ones duties or job function. For example, it is acceptable to use software to make a flyer for an employee reception, but not acceptable to use software for designing artwork for your bedroom wall.

2. Scope.

This policy applies to: All software-produced data.

3. Policy.

- A. Software licensed for City use is the only software that may be loaded or downloaded onto the System. The unauthorized copying of City licensed software, installation or use of unlicensed software ("Pirated Software"), or the modification of Software licensed for city use for installation and/or use on non-city owned computers or hardware is expressly prohibited.
- B. All diskettes shall be scanned for viruses before accessing data stored on the disk. This includes diskettes received from any source (internal or external).
- C. The City has established standard software applications for general use. Any software not on the list of standard software must be approved for use by the System Administrator. Justification should include what special purpose the software is needed for. A list of current software systems can be found in Addendum A.

Password Security Policy

1. Policy.

- A. While much information at City Hall is public information, several City Departments are required to protect citizen's rights to privacy. Therefore, all City systems will be login and password protected. This will protect citizens and hopefully avoid potential "hacking" or tampering with information on City computer systems. Where warranted, security "firewalls" will be implemented to maintain system security.
- B. Passwords are required for ALL accounts on any system.
- C. Users will be required to change their system when instructed to do so.

- D. Unique passwords are required so that users cannot repeatedly use the same password.
- E. Standards for monitoring security and potential breaches are implemented on each computer system to ensure security of the enterprise.
- F. Don't give your password to a co-worker or supervisor. Remember you are responsible for all information that is accessed while logged on. If he/she asks for your password say "NO". You have that right. Don't let a co-worker or supervisor use your password. If a coworker forgets his or her password, and you allow that person to access information under your password, you are responsible for his or her actions because the information is being accessed under your password. The ONLY exception to this is for the designated System Administrator to need access to passwords to configure a new program. This is necessary due to the permissions for that particular employee's access to the network.
- G. Employees are responsible for the security of their system. You shouldn't leave your workstation unattended without logging out or adding a password protection. It only takes a minute for someone to access critical information from your workstation. Once again, it's your password that's accessing information.
- H. The System Administrator or designee will be allowed to remove network or system users when needed for personnel reasons (This is necessary if a personnel action might cause a security risk).

Printers Policy

1. Definitions.

The following definitions apply through this policy:

- a. Printer. A device which allows a computer user to print data onto paper.
- b. Hardware. Hardware in this case includes not only the physical printer but also the cables, connectors, and power supply units.
- c. Consumables. Components associated with printers which require frequent replacement (e.g. paper, toner).

2. Policy.

- A. Shared, network printers will be implemented wherever feasible. Personal printers will be allowed only with justification and to address confidentiality or other specific issues. Requests by Department Heads for individual printers will be reviewed on a case-by-case basis with the IS Manager.
- B. The IS Manager will establish protocols for acceptable length of print jobs, use of recycled paper/banners, use of recycled print cartridges, printing confidential material to shared printers, etc.