CITY OF FREMONT
COMPUTER USE AND DATA ACCESS POLICIES

I. INTRODUCTION

The City of Fremont maintains its computer system and network for official purposes only. This computer hardware, software and data protection policy reflects the position of the City of Fremont regarding the use of hardware, software and data in all City offices and departments.

Scope

This policy applies to employees working for the City of Fremont on a full-time, part-time, probationary, temporary or seasonal basis. It refers to all information resources owned or under control of the City, whether individually controlled or shared. Information resources include any information in electronic or audio-visual format, or any hardware or software that makes possible the storage and use of information. Included in this definition are electronic mail, local databases, externally accessed databases, all City-controlled web sites, CD-ROM, digitized video and photographs and all other digitized information.

II. DATA PROTECTION POLICY STATEMENT

The City of Fremont depends heavily on computer use and information to conduct its business. It is essential that this information be accurate and protected from unauthorized destruction, modification or disclosure.

When using City computers, employees must adhere to the same code of ethics and personnel policies that govern all other aspects of City government as contained in the City's Personnel Policies Manual. Any actions performed or initiated through the City computer system must be done with integrity, honesty, and compliance with the City’s rules of conduct.

The following rules for computer and data use are intended to supplement existing personnel policies by clarifying the expected conduct of employees when working with computers and computer data. If you have a question concerning any computer policy or its application, consult System Administration (i.e.- City Clerk or City Manager.)

III. AUTHORIZED USE

The City provides computing resources to accomplish tasks related to the City’s mission. These include correspondence, record keeping, administrative support activities, database access and maintenance and other uses specified by an employee’s supervisor or job description.

IV. RESTRICTIONS

- All employees must use City computer resources solely for purposes for which they have been authorized. Computing resources may be connected to the Internet or a department or City...
network for the performance of authorized tasks. Accessing or attempting to access computer resources, the Internet or network to perform unauthorized tasks is not permitted.

- Using a computer to access the accounts and files of others or to alter the work product of others without permission is prohibited.

- Attempting to subvert network security, impair functionality of the network or bypass restrictions set by administrators is prohibited. Assisting others in violating these rules by sharing information or passwords is also prohibited.

- The improper use or distribution of City owned data or information is prohibited.

- The unauthorized use of computer resources, as well as providing false or misleading information for the purpose of obtaining access to computing facilities, is prohibited. Employees shall not gain unauthorized access to City computing facilities or use City computer resources to gain unauthorized access to other institutions, organizations or individual computers.

- Employees must take all reasonable precautions, such as password maintenance and file protection measures, to prevent the use of his/her computer by unauthorized persons. Employees must not, for example, share a password or dial-in access number with any unauthorized person.

- City computer resources may not be used for non-work purposes, commercial activities, financial gain or entertainment.

- All employees who have been authorized to use City computing resources shall regard all personal or proprietary information, which may thereby become available to him/her as confidential.

- Employees shall not copy system files or attempt to access or modify such files, software, computer management programs or data except when authorized to do so by System Administration.

- Employees shall not attempt to modify or repair any computer equipment belonging to or under the control of the City unless authorized to do so by System Administration.

- City computer equipment shall remain on City premises at all times, with the exception of laptop computers assigned for field use and other exceptions authorized by System Administration.

- No employee shall install or use any encryption program unless specifically told to do so by System Administration.
V. SPECIFIC POLICY ELEMENTS

A. Physical Protection of Information and Equipment

- All computer equipment is to be secured as best as possible when not in use or left unattended. Laptop computers shall not be left in unlocked vehicles.

- All non-server computers shall be logged off upon completion of use or at the end of the work shift.

- The security of non-assigned computers shall be protected by logging off at the end of the work shift.

B. Deleting Data or Information

The department head or System Administration shall approve all information or data that is removed from the computer. No information shall be permanently deleted from the system without prior authorization. Individual departments may authorize the routine deletion of specific categories of information if individual departments establish back-up and archiving procedures for the retention of deleted data.

C. Remote Access Policy

Remote access to City computers by officers, employees and vendors shall be by prior approval of the System Administration.

D. E-mail

- E-mail is to be used for conducting only City business. E-mail is not to be used as a form of entertainment or as a forum for political, religious or any other personal expression inconsistent with work place responsibilities.

- The e-mail system and its contents are the property of the City of Fremont and employees have no expectation of privacy in its use or content. For example, a single e-mail message sent to just one person can be forwarded, without permission of the sender, to hundreds of others either intentionally or inadvertently. E-mail exchanges are subject to release under the State's Freedom of Information Act (FOIA).

- Although there is no expectation of privacy in City e-mail, no City employee is to use his or her position or access rights to read another employee's e-mail or personal files. The only people authorized to do this are individual department heads. System Administration may also, in consultation with affected department head(s), direct authorized persons to access individual e-mail accounts.
• E-mail may not be used to send harassing, threatening or offensive messages. Sexual or bigoted material is prohibited. Employees must always bear in mind the standards of professional conduct.

• In light of worm viruses such as “I Love You” and “Melissa”, no employee shall open any attachment to an e-mail unless the attachment is one specifically requested by the employee from the sender. Under no circumstances shall an employee open an attachment from an unknown sender. If an employee receives e-mail with an attached file from a known sender but has not requested or is not expecting it, he/she shall contact the sender either by e-mail or telephone to verify the content of the attachment before opening.

• Any file attached to e-mail sent by another City employee shall be preceded with an e-mail advising the recipient that an attachment has been forwarded and including a brief description of the file.

E. Privacy Rights and Limitations

No privacy rights exist to any personal files or e-mail created or received on City computer resources. As stated previously, City computer equipment is to be used to conduct City business and therefore any personal information stored or created on this equipment is subject to review and elimination by appropriate authorities.

The City of Fremont is a governmental unit and is therefore subject to the State's Freedom of Information Act (FOIA). As such, electronic information and e-mail created in the performance of employee job duties may be considered a public record. Therefore, all computer files generated by City officers and employees are subject to review and possible release. Even personal e-mail or files not related to the specific issue discussed in the FOIA request may be examined in the course of responding to a FOIA request.

System Administrators or other City personnel may also need to gather information from computers to ensure the continued functioning of computer resources or to investigate complaints. This may require the examination of activity logs, files, e-mail and printer listings to gather information necessary to diagnose and correct problems with system software or hardware. Individual computer files may also be examined to determine if policy violations have occurred or are occurring.

Privacy policies contained in other City documents should also be followed when working with computer data.

F. Password

• The purpose of passwords is to protect the City’s database and information from corruption or use by unauthorized individuals.
• All passwords are considered confidential information and may not be disclosed. A password may not be used by anyone other than the person(s) who has been authorized to use it.

• All employees must notify their department head or supervisor if they believe their password is being used or has been compromised by others.

• All employees shall leave their password in a sealed envelope with System Administration to be stored for security measures. These passwords will be accessed only in the event of an emergency and the employee will be notified. The employee may then decide whether to change their password. A sealed envelope containing the new password with the employee’s name and date on the envelope must be re-submitted any time that their password is changed.

G. Virus Protection

• City computers should be protected by software that scans for viruses. Virus detection helps avoid destruction of computer files and hard drives. However, since virus protection software is not 100% effective, it is extremely important to follow procedures to protect computer data. This is an important issue and if a damaging virus were to destroy a hard drive’s contents the cost to the City of Fremont could be thousands of dollars.

• The installation and use of software on City computers, not owned by the City, is prohibited without authorization from System Administration.

• Virus scanning programs shall not be disabled without authorization from System Administration.

H. Network Security

Network security is dependent on employees. Each employee or group of employees has a set of specific rights on individual computers and file servers. Each department may establish employee privileges based on an employee’s job function. The department head, supervisor or System Administrator may define specific user groups and access privileges. These access privileges determine which files or data an employee may access.

I. Software Use

The City forbids, under any circumstances, the unauthorized reproduction of software or use of illegally obtained software. Using City equipment to make illegal copies of software is prohibited. City employees who violate this policy are subject to disciplinary action and/or legal action by the City. Individuals who violate U.S. copyright law and software licensing agreements may also be subject to criminal or civil legal action.
City employees are required to follow conditions or restrictions required by the licensing agreements for software programs purchased by the City.

J. Internet Use

Internet access from City computers is to be used for City business. Individual departments may authorize and define business use, subject to System Administration approval.

No program or application shall be downloaded from the Internet and installed on City computers without prior permission of System Administration.

VI. RESPONSIBILITIES AND CONSEQUENCES OF NON-COMPLIANCE

All City employees are expected to comply with this policy. Any employee who violates this policy is subject to disciplinary action consistent with personnel policies and may also be subject to criminal or civil prosecution under applicable laws.

Any employee who has reason to believe that a coworker may be misusing City computer resources or violating any aspect of this policy shall voice his/her concern to his/her department head or System Administrator. Department heads are responsible for addressing any policy violations of which they become aware. Department heads may refer the matter to System Administration if appropriate.

Adopted by the
Fremont City Council
June 19, 2000
POLICE DEPARTMENT INTERNET POLICY

I. PURPOSE

The purpose of this procedure is to provide guidelines for access and use of the Police Department’s Internet, E-mail, and car to car messaging (CTCM) systems.

Note: The City of Fremont has adopted Personnel Policy 39 “Computer Usage,” which has been distributed to all employees. The provisions of the City of Fremont policy must be followed by all employees unless modified by the Chief of Police.

II. INTRODUCTION

A. The use of the Internet, E-mail, and CTCM is becoming increasingly necessary for municipal employees to provide superior customer service and for enhanced intra/inter agency communication. The efficient use of these systems for communications and research can improve the quality and productivity of the services the City provides to the citizens of Fremont.

B. The Police Department’s Internet, E-mail, and CTCM access is a privilege granted to employees to enhance their abilities and knowledge, increase their productivity, and provide opportunities for personal and professional growth.

C. Remember, when you are conducting business on the Internet, E-mail and CTCM systems, you are representing the City of Fremont. Therefore, all actions and communications will be conducted in a lawful, courteous and ethical manner.

III. INTERNET ACCESS

A. Requests for Internet and E-mail access should be directed to your Division Commander. The Division Commander will contact Automated Data Operations (ADO) to authorize approved requests.

B. Once the new user has participated in the basic ADO Internet course, Internet software will be loaded and appropriate password(s) established for the user’s computer.

C. A screen saver password will be utilized on all computers able to access the Internet.

D. ADO will maintain a list of all current Internet Stations and E-mail accounts.

IV. DEPARTMENT COMPUTER USE POLICIES

The Police Department has the authority to develop policies for computer, Internet, E-mail and CTCM use to address particular departmental needs under the provisions of Personnel Policy 39 “Computer Usage.” Any Police Department policies developed will be developed in accordance with the City policy.
V. INTERNET CONTENT CAUTION

A. A wide variety of information is available on the Internet. Individuals may find some information on the Internet offensive or otherwise objectionable.

B. Individual users should be aware that the City has no control over and can therefore not be responsible for the content of information available on the Internet.

VI. VIRUSES

A. Many of the sites available on the Internet such as Bulletin Boards can be breeding grounds for computer viruses. If these viruses are downloaded on a City Network and are not detected, they may contaminate City information systems and databases.

B. Any and all material downloaded from the Internet will be downloaded to the user’s local hard drive only (C: Drive). No downloaded Internet files will be copied to any Police Department or City network drive.

C. All downloaded files must be scanned manually or automatically for computer viruses. If a virus is detected, ADO shall be notified immediately.

VII. SECURITY/PASSWORDS

A. The safety and security of the Police Department’s computer networks and resources must be considered paramount when using the Internet.

B. User passwords are confidential. Therefore, it is the user's responsibility to maintain the confidentiality of all password(s).

C. All non-server computers shall be logged off upon completion of use or at the end of the workday with the exception of those computers assigned to 24 hour a day operations that are secure from unauthorized users.

VIII. OPERATION RULES

A. All access to the Internet, E-mail and CTCM by employees working for the Police Department on a permanent or temporary basis, shall be done in a professional manner and in compliance with all applicable laws and City policies.

B. The Internet is a valuable resource tool. Employees are encouraged to use the Internet in the performance of their duties, or to enhance their effectiveness. However, users shall not “Surf the Net” on topics unrelated to the performance of their duties during work hours.

C. Internet use, E-mail received and sent, CTCM, and all City databases can be monitored and are the property of the City of Fremont.
D. Internet use, CTCM, individual computer files, E-mail messages or other information contained in Police Department computers, servers, or software are subject to review and/or audit by the Police Department.

E. No Employee shall use the Internet, E-mail, or CTCM systems for mass distribution of personal or non-business information.

F. No Internet, E-mail, or CTCM system shall be used to send copies of any documents or files violating copyright laws.

G. No program or application shall be downloaded from the Internet and installed on Police Department or City computers without the prior permission of your Division Commander or ADO.

H. The Internet, E-mail, and CTCM shall not be used for any illegal, improper, unprofessional or illicit purposes. Intentional misuse may subject the user to termination of access privileges and/or disciplinary action.

VII. RESPONSIBILITY

It shall be the responsibility of all personnel to know and comply with this procedure.