Computer System Protocols

1. Software

Protocol: The use of computer software is an integral part of most city operations. Each computer will be equipped with a standard set of computer applications.

Purpose: To insure maximum productivity and efficiency, and to make system maintenance as efficient as possible, installing a standard set of basic software tools is beneficial. When standardized software packages are used, it makes the electronic exchange of documents, and training, simpler. Installation of specialized software may be authorized after review by the IT Department.

Steps to Compliance:

1) Each computer will have a minimum software configuration package which includes: Microsoft Windows 2000 Professional, Microsoft Office XP Professional (including word processor, spreadsheet, and presentation program), and Networking Package (when connected to a network).

2) Upgrades to installed software shall be made on a Division, Department, or Citywide basis.

3) All software will be purchased and used in compliance with the licensing agreement provided by the software vendor.

4) IT Policy purchasing procedures shall be followed when obtaining software.

5) Only software approved for installation on a city computer shall be used. Such software includes the City's approved operating system, approved office suite, approved email/internet applications, and other approved applications.

Computer System Protocols

2.   Electronic Messaging (E-Mail)

Protocol: E-Mail is a tool for conducting business related activity. E-Mail is defined as any form of electronic communication on or over City owned computer equipment. It includes, but is not limited to, electronic messages, electronic calendaring, notes, faxes or attachments.

Purpose: The purpose of this policy is to establish guidelines for the proper use and application of electronic mail (e-mail) by employees of the City of Ceres. E-mail is a communication tool available to City employees to enhance the efficiency in the performance of job duties and is to be used in accordance with generally accepted business practices and current law (e.g. California Public Records Act). City e-mail should be used primarily for City business. The use of E-mail as a workplace tool creates new concerns for employee privacy rights, the rights of third parties to obtain access to E-mail records, and the placement of E-mail records in an employees personnel file. Consistent policies are necessary because the improper use of E-mail by employees not only wastes public resources, but also exposes the City to potential liability.

E-MAIL RIGHT OF PRIVACY

All e-mail messages transmitted over the computer network are considered City records and, therefore, the property of the City of Ceres. The City reserves the right to access, audit and disclose all messages transmitted over its e-mail system or placed into its storage.

The e-mail system is not a confidential system since all communications transmitted on the system are the property of the City. Therefore, the e-mail system may not be appropriate for confidential communications. If a communication must be private, an alternative method to communicate the message should be used instead of e-mail. Employees using the Department's e-mail system should have no expectation of privacy concerning communications in the system.

Disclosure of information or messages from the E-mail systems should only be made to authorized persons. Public Safety employees are responsible for knowing California Department of Justice policies and procedures restricting the release of DOJ-controlled information. Public Safety employees also are responsible for knowing federal policies and procedures restricting the release of federally controlled law enforcement information.

Computer System Protocols

PROHIBITED USE OF E-MAIL

Improper use of electronic mail includes, but is not limited to the following and is strictly prohibited:
- Sending or opening anonymous e-mail (defined as e-mail which does not clearly identity the sending individual, company, department, etc.) is prohibited.
- Theft and/or forgery (or attempted forgery) of e-mail messages or electronic documents.
- Unauthorized access, deletion, copying or modifying another employee's e-mail
- Any attempts to send unsolicited junk mail, for-profit messages, chain letters, pornography, or other inappropriate mail that could be considered offensive.
- Conducting any type of personal, outside employment, paid services, or advertising on City time and through City systems
- Sending religious or political messages or announcements

MANAGEMENT OF E-MAIL

The e-mail system is not designed for long-term retention of messages; e-mail that the employee desires to save or that becomes part of an official record should be printed. Users of e-mail are solely responsible for the management of their mailboxes. Routine messages should be purged manually by the user at least once per week. Important messages may be archived. When you decide to archive a message, remember that everything stored on your desktop computer is public record and may be subpoenaed at any time.

Your e-mail address is owned by the City of Ceres, and care should be given as to whom you give it out to. When the confidentiality of information is unclear, it should not be divulged. Disclosure of information or messages from the E-mail systems should only be made to authorized persons.

Simply deleting e-mail will not erase it from the system. E-mail must also be removed from the e-mail client's deleted folder. If you don't know how to do this, please call the IT Department and we'll give you a brief demonstration.

3.   Software Installation

Protocol: Software installed on a City computer requires the approval of the IT Supervisor and a Department Head.

Purpose: Any software installed on a city computer becomes the property of the City. Because of the potential for an inexperienced user to cause damage to the operating system or computer software configuration when

installing software, only IT employees will install software, (rare exceptions may be made). The loss of a computer for even a short time can create a significant (and costly) hardship for the employee, and most importantly, to a City customer. Approval by the IT Department is important so that we may be assured of compliance with our systems, equipment and configuration.

DEFINITIONS: The following definitions relate to terms used within this policy:

"Computer System" shall mean all computers (on-site and portable), hardware, software, and resources owned, leased, rented, or licensed by the City of Ceres, which are provided for official use by City employees.

"Hardware" shall include, but is not limited to, computers, computer terminals, network equipment, modems or any other tangible computer device generally understood to comprise hardware.

"Software" shall include, but is not limited to, all computer programs and applications including "shareware." This does not include files created by the individual user.

"Temporary or Permanent File" or **"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, notes, letters, reports or messages.

SYSTEM INSPECTION OR REVIEW

An employee's supervisor, department head, or the city's IT staff have the authority to inspect or review the System, all temporary or permanent files and related electronic systems or devices, and any contents thereof when such inspection or review is in the ordinary course of his/her supervisory duties.

When requested by an employee's supervisor, department head, or the city's IT staff ,or during the course of regular duties requiring such information, a member(s) of the City's Information Technology staff (IT.) may extract, download, or otherwise obtain all temporary or permanent files residing or located in or on the System.

Reasons for inspection or review may include, but are not limited to: system malfunctions, problems or general system failure, a lawsuit against the City involving the employee or related to the employee's duties, an alleged or suspected violation of the City policy, or a need to perform or provide a service when the employee is unavailable.

Computer System Protocols

CITY PROPERTY

All information, data, documents and other entries initiated on any of the City of Ceres computers, whether downloaded or transferred from the original City computer, shall remain the exclusive property of the City of Ceres and shall not be available for personal or non-departmental use without the expressed authorization of an employee's supervisor.

UNAUTHORIZED DUPLICATION OF SOFTWARE

Users should notify IT Department Staff and receive proper authorization from their supervisor before attempting to copy software. In many cases, copyright laws and/or licenses for commercial software, programs, applications, and templates used by the City prohibit making multiple copies. Usually, software licenses permit a single copy for backup purposes. The City and its employees are required to abide by the federal copyright laws and to abide by all software licensing agreements. To reduce the risk of personal computer virus infection, employees are not permitted to install personal copies of any software onto the City's computers. If an employee must copy data onto a disk and download it on a non-City computer, the employee shall scan the disk for viruses before reloading the data on a City computer system.

No employee shall knowingly make, acquire, or use unauthorized copies of computer software not licensed to the City while on City premises or on a City computer system. The City and individuals can be subject to civil damages of as much as $150,000 per title copied, along with criminal penalties including fines up to $250,000 and imprisonment for up to five years. Employees can personally suffer both civil and criminal penalties for violating software copyright laws.

INTERNET USE

Internet access provided by the City of Ceres should be used primarily for City business. Internet sites containing information that is not appropriate or applicable to departmental use and which shall not be intentionally accessed include, but is not limited to, adult forums, pornography, "chat rooms," and similar or related web sites.

Downloaded information shall be limited to messages, mail, and data files. No copyrighted and/or unlicensed software program files shall be downloaded, including music files and movie files.

Employees shall report any unauthorized access to the System, or suspected intrusion from outside sources (including the Internet), to a supervisor and IT staff.

Computer System Protocols

PROTECTION OF CITY SYSTEMS AND FILES

All employees have a duty to protect the System and related systems and devices from physical and environmental damage, and are responsible for the correct use, operation, care, and maintenance of the System.

It is expressly prohibited for any employee to allow an unauthorized user to access the System at any time or for any reason. Generally, anyone who is not a city employee is an unauthorized user. An exception would be made for a contractor. Another city employee may also be an unauthorized user if you allow him/her to access your system while it is logged in under your username, and your username gives him/her rights to areas of the network they would not have under their own username. To prevent this from happening, log off your system before allowing another employee to use it.

Steps to Compliance:

1) Get approval from the IT Supervisor or authorized personnel for any software installation.

2) Contact an IT representative to schedule installation.

3) An IT representative will scan software for viruses prior to installation.

4) The Department and/or IT representative will be responsible for collecting, and retaining, the software, licensing and associated manuals for future reference. The IT Department will maintain a listing of all software utilized by departments and/or divisions.

5) Third party Screen Savers are not permitted due to performance issues. They will be removed.

4.   General Usage

- Network users should routinely log out of the network or lock the workstation when away from their workstations for an extended period. This is a security issue.

- At the close of a network user's day, he/she must log out of the network for security purposes. Turn off all computer related equipment, including the PC, the monitor, and printer, etc. over weekends, vacations or extended periods of absence.

<u>Computer System Protocols</u>

- Employees should save files to the network, not to their C:\ drives. Network storage for worker data is strongly encouraged - doing so protects against unauthorized access to data and provides a level of protection against data loss. It is the user's responsibility to routinely save their files to the network.

- Network passwords should not be shared with others and should be changed at least annually. If you wish to change your password, please contact an IT representative.

- Internet access users should limit their use of the Internet to brief periods. Use of the Internet to listen to music or watch movies is not allowed. These uses limit our bandwidth and slow access to the Internet for the rest of the network users.

- If you are experiencing problems with your PC, do not wait to seek help or allow problems to accumulate to be fixed all at once. **YOU ARE NOT BOTHERING US.** Computer support staff wants to help whenever we can to make your job easier. Give us a chance to fix the problems as they arise.

- Before requesting help, try some basic recovery methods on your own. Make sure power is on to the PC, monitor, and peripheral equipment attached to your PC. Make sure to exit Windows properly and shut down your PC, ("cold start"), and see if this fixes the problem. Empty the "RECYCLE BIN" on your Windows desktop on a regular basis. These procedures are designed to keep your PC running smoothly.

- Keep a "want" list of things that would make your job easier and more efficient if you had them installed on your PC, and regularly pass them along to the IT Department.

The Ten Rules of City Computer Usage

1) No software of any kind shall be installed on a City computer without the review of the IT department.

2) Software shall only be installed on city computers by an IT representative, or an authorized representative.

3) The use of City computers and software shall be governed by the adopted City IT Policy. Failure to abide by the adopted policy may be cause for discipline as outlined in the City's Personnel Policy.

Computer System Protocols

4) The security of documents that are of a sensitive nature, or require special security considerations, cannot be guaranteed when stored on your city computer, or on the network server. While the city strives to make systems and servers as secure as possible, both might be compromised by unauthorized users (burglars, contractors, employees who work at night) or hackers. Even password protected documents are not secure. If a document must be absolutely secure, make sure it exists only on paper and store it in a safe.

5) Employees shall not use a co-workers network password. All users shall have a unique account.

6) Requests for routine system maintenance should be submitted to the IT Department. Routine maintenance includes such things as software glitches and printing problems, minor issues that pop up during the course of an average work day. Employees shall direct all requests for non-routine maintenance services through the IT department. Non-routine maintenance includes such things hardware/software installation, network modifications, repairing physical damage to equipment, etc.

7) Employees must not open files on a computer disk brought from home, or obtained from an outside source, without first scanning for the presence of computer viruses. If you don't know how to scan for viruses, contact the IT Department and they will scan it for you.

8) When in doubt, about any interpretation of these policies, or other issues related to the use or operation of City computer hardware or software, employees should contact a supervisor or an IT representative for direction.

9) Write down any error messages that pop up on your monitor when problems occur. This will help IT staff with troubleshooting.

10) When experiencing minor problems, close all programs and shut down your computer. Seventy percent of the time this will solve your problem.