City of Sterling
Personnel Policies

Effective Date: January 1, 2009		# of Pages: 7
Rev. Effective Date:		
Personnel Board Approval		Date
Board President	Marcus J. Floyd	6/30/11
Board Member	Edward A. Baker	
Board Member	Ted E. Johnson	6-30-11

CHAPTER 19
GENERAL POLICIES

SECTION 1 – IDENTIFICATION CARDS

The City has the ability to provide "City Identification" card to employees whom the City Manager deems advisable. The I.D. card is given to the employee for the purpose of personal identification and to illustrate their relationship with the City. Misuse of the card such as for personal gain and fraudulent purposes, will be reason for dismissal. If the I.D. Card is lost, it shall be reported immediately to the Department Head or supervisor. Failure to do so is subject to disciplinary action.

The I.D. card is the property of the City and must be surrendered immediately upon separation from employment.

SECTION 2 - POLITICAL ACTIVITY

(a) It is the duty and right of every employee to register and vote on all political issues. Employees are permitted to join political organizations, civic associations, or civic betterment groups.

(b) Employees are not permitted to engage in any political activity involving the election of candidates for any City office during on-duty hours.

(c) Any employee desiring to become a candidate for City elective office shall first resign. Should such employee be unsuccessful in seeking office, they may be returned to employment on the same terms as any other employee who has taken a leave of absence without pay, provided the position is vacant after the election outcome.

(d) Employees are not permitted to solicit, sell, or handle political contributions in City elections. Employees are not permitted to wear or display political badges, buttons, or signs on their person during on-duty hours.

SECTION 3 - MEMBERSHIP ON BOARDS AND COMMISSIONS

Employees, except temporary and seasonal persons and elected officials, are not permitted to be a member of Council, boards, or commissions that are advisory or administrative to the City, except where such membership is specifically authorized by City ordinance.

City of Sterling
Personnel Policies

SECTION 4 - OUTSIDE EMPLOYMENT

This section applies to all regular full, partial and part time appointments. With the financial commitment made to employees through the benefits package for these types of appointments, the City of Sterling shall be considered as the primary employer for individuals seeking secondary employment or becoming self employed. As a result of this, employees may engage in outside employment or self employment outside normal duty hours if:

(1) There is no conflict in working hours;

(2) The employee's efficiency or effectiveness is not reduced by secondary employment;

(3) There is no conflict of interest arising out of secondary employment (See **SECTION 5** of this chapter); and

(4) A request of intent of secondary employment is made in writing and reviewed then either approved or denied by the employee's Department Head and the City Manager. Any denial of secondary employment by the City Manager regardless of the decision of the Department Head is final.

SECTION 5 - CONFLICT OF INTEREST

No employee shall engage in any activity or enterprise which conflicts with his duties as a City employee or with the duties, functions, and responsibilities of the department in which employed. The following activities shall be considered a conflict of interest with City employment:

Any employment, activity or enterprise which:

(a) Involves the use, for private gain, of the City's time, facilities, equipment, or supplies;

(b) Involves the receipt or acceptance of any money or other consideration from anyone other than the City for performance of an act which would be expected to be rendered in the regular course of City employment or as part of the duties of a City employee;

(c) Involves the performance of an act in other than the capacity as a City employee which may later be subject, directly or indirectly, to the control, inspection, review, audit, or enforcement by such employee or the employee's department; or

(d) Involves so much of the employee's time that it appears that the employee's attendance or efficiency in the performance of duties as a City employee is impaired.

SECTION 6 - RELEASE OF CITY INFORMATION TO NEWS MEDIA

News information from City Departments will be released in accordance with established policies and procedures regarding dissemination of information adopted by the department and approved by the City Manager. No City employee is to make any type of a "news" release to any form of news media concerning city operations, business matters, etc., unless authorized to do so in compliance with adopted departmental operational policies and procedures. Normally news releases will be made from the City Manager's or City Attorney's office.

City of Sterling
Personnel Policies

SECTION 7 - SAFETY

NOTE: Disobeying a safety rule may result in disciplinary action up to and including discharge and, as provided in C.R.S. §8-42-112(1), may also result in the reduction of any workers' compensation benefits that would otherwise be available to an employee who suffers a work-related injury as a result of the violation of a safety policy.

A. General Safety Rules

The following lists only some of the key safety rules; the list is not intended to be exhaustive or all-inclusive. Each department may prepare separate safety rules applicable to the specific nature of work in their area but not in conflict with these rules.

- Proper training and extreme caution are required by all employees operating any type of power equipment.
- Employees will use personal protective equipment appropriate to the job, such as safety glasses, gloves, safety shoes, and hard hats, if required or appropriate to the work performed.
- Employees will avoid wearing loose clothing and jewelry while working on or near equipment and machines.
- All accidents, regardless of severity, personal or vehicular, are to be reported immediately to the employee's supervisor.
- Defective equipment must be reported immediately to the supervisor.
- Supervisors will conduct a safety inspection at least annually of significant operations and properties.
- Employees will not operate equipment or use tools for which appropriate training has not been received.
- Material Safety Data Sheets (MSDS) will be made available to employees handling materials to which such MSDS pertain.
- Proper trenching and excavation procedures will be followed by employees involved in such operations.
- Proper confined space entry procedures will be followed by employees involved in such operations.
- Work zone protection will be utilized when work is performed on a public way.
- Employees are encouraged to think about how to make their workplace safer for both themselves and their coworkers. Suggestions on improving safety at the City/Town are welcomed and should be directed to the employee's supervisor.
- Employees will be evaluated on their safety performance as part of their overall performance evaluation.

B. Safety Committee

Depending upon insurance carrier loss control standards, it is the prerogative of the City Manager to staff a Safety Committee. The City Manager shall have the discretion to make employee assignments to serve on such a safety committee. The City manager may also cause to be formed various subcommittees from the members if it is advisable based on insurer loss control standards.

The Safety Committee is charged with recommending City Safety Rules, coordinating activities and rule making with the City insurer loss control personnel to meet industry best practices, and to train city employees in compliance with the City's Safety Rules. Safety Rules are subject to City Manager approval and adoption. It shall be the responsibility of each employee to read, understand and apply all City safety rules.

SECTION 8 – ELECTRONIC COMMUNICATIONS

A. Electronic Communications Policy

This policy governs the use of computers, networks, and related services of the City. Users of these resources are responsible for reading, understanding, and complying with this policy. Computers and networks can provide access to resources within and outside the City, as well as the ability to communicate with other users worldwide. Such access is a privilege and requires that individual users act responsibly.

Users must respect the rights of others, respect the integrity of the computers, networks, and related services, and observe all relevant laws, regulations, contractual obligations, and City policies and procedures. Misuse of the City Computer System can undermine public confidence and waste taxpayer resources.

B. The City Computer System

The City Computer System includes: computers and related equipment, e-mail, telephones, voice mail, facsimile systems, communications networks, computer accounts, internet and/or web access, network access, central computing and telecommunications facilities, and related services.

Access to and use of the City Computer System is a privilege granted to City staff. All users of the Computer System must act responsibly and maintain the integrity of the Computer System. The City reserves the right to deny, limit, revoke, or extend computing privileges and access to the Computer System in its discretion.

The City may, in its discretion, limit the use of specified portions of the Computer System to certain employees, and/or deny the use of specified portions of the Computer System to certain employees.

The City Computer System may not be used in any manner or for any purpose which is illegal, dishonest, disruptive, threatening, is damaging to the reputation of City, is inconsistent with the mission of the City, or could subject City to liability.

Any violation of this policy or of other City policies in the course of using the Computer System may result in an immediate loss of computing privileges, disciplinary action up to and including termination of employment, and referral of the matter to the appropriate authorities.

C. No Expectation of Privacy

City personnel have no expectation of privacy in City property and equipment. Such property and equipment includes, but is not limited to, the City Computer System, and all messages, data files and programs stored in or transmitted via the Computer System ("Electronic Communications"). City reserves the right to monitor, access, use, and disclose all messages, data files and programs sent over or stored in its Computer System for any purpose. City management reserves the right to monitor, inspect, and examine any portion of the Computer System at any time and without notice.

The City may monitor or access an employee's e-mail, with or without notice, for any business-related purpose, including any situation in which a supervisor has reason to believe that an employee is misusing or abusing e-mail privileges, or is violating any other City policy.

Further, correspondence of an employee in the form of e-mail may be a public record under the public records law, and may be subject to public inspection under C.R.S. Section 24-72-203, unless an exception provided by law applies.

D. Passwords

Portions of the City Computer System may be accessible by password only. The purpose of a password is not to provide privacy, but to control and prevent unauthorized access.

Every password issued for the use of any part of the City Computer System is the responsibility of the person in whose name it is issued. That individual must keep the account secure from unauthorized access by keeping the password secret, by changing the password often, and by reporting to the City when anyone else is using the password without permission. Passwords not provided by the City, but generated by the user, must be provided to the City's IT Department.

Passwords are intended to help prevent unauthorized access and may not be shared with unauthorized persons. The contents of all password protected data files and programs belong to the City and are subject to access and disclosure by the City as set forth in this policy.

E. Remote Access

Off-site access to the City electronic communications systems may be granted on a limited basis by the City Manager. An employee using a non-city owned device to access the City's system shall be responsible for any viruses, malware, etc., which may be transmitted through the connection of a private personal communications device. Uploading information from a personal communications device to the City electronic system may only occur after the written approval of the IT Specialist. Once the uploaded information is in the City system, all elements found in this policy shall apply.

F. Improper Use of the Computer System.

Improper use of the Computer System is prohibited. The following are examples of the improper use of the Computer System:

- **Storage, Transmission, or Printing of Improper Materials:** Storing, transmitting or printing any of the following types of Electronic Communications on the Computer System is prohibited: material that infringes upon the rights of another person; material that is obscene; material that consists of any advertisements for commercial enterprises; material or behaviors that violate laws, regulations, contractual obligations, and City policies and procedures; or material that may injure someone else and/or lead to a lawsuit or criminal charges.
- **Harassment:** Any electronic communication that violates the City harassment policy is prohibited. Additionally, any electronic communication that is abusive, profane, threatening, defamatory or offensive is prohibited. Some examples include: obscene, threatening, or repeated unnecessary messages; sexually, ethnically, racially, or religiously offensive messages; and continuing to send messages after a request to stop.
- **Destruction, Sabotage:** Intentionally destroying anything stored on the Computer System, including anything stored in primary or random access memory is prohibited. Deliberately performing any act that will seriously impact the operation of the Computer System is also prohibited. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer or peripheral.
- **Evasive Techniques:** Attempts to avoid detection of improper or illegal behavior by encrypting or passwording electronic messages and computer files are prohibited.
- **Unauthorized Use/Access:** Using the Computer System to gain or attempt to gain unauthorized access to remote computers is prohibited. Other prohibited behaviors include: actions that give simulated sign off messages, public announcements, or other fraudulent system responses; possessing or changing system control information (e.g., program status, protection codes, and accounting information), especially when used to defraud others, obtain passwords, gain access to and/or copy other user's electronic communications, or otherwise interfere with or destroy the work of other users.
- **E-Mail Forgery:** Forging e-mail, including concealment of the sender's identity, is prohibited.
- **Theft/Unauthorized Use of Data:** Data created and maintained by the City, or acquired from outside sources, are vital assets of the City and must be used only for authorized purposes. Theft of or unauthorized access to or use of data is prohibited.
- **Program Theft:** Unless specifically authorized, copying computer program(s) from the Computer System is prohibited.
- **Viruses, etc:** Intentionally running or installing on the Computer System, or giving to another, a program that could result in damage to a file or the Computer System, and/or the reproduction or transmission of itself, is prohibited. This prohibition includes, but is not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.
- **Security:** Attempting to circumvent data protection schemes or uncover security loopholes is prohibited.
- **Wasting Resources:** Performing acts that are wasteful of computing resources or that unfairly monopolize resources to the exclusion of others is prohibited. These acts include, but are not limited to: sending mass mailings or chain letters; creating unnecessary multiple

jobs or processes; generating unnecessary or excessive output or printing; or, creating unnecessary network traffic.

- **Personal use:** It is understood that, occasionally, employees use e-mail or internet access for non-commercial, personal use. Such occasional non-commercial uses are permitted in conformity with any guidelines or requirements established by the department head, do not interfere with the performance of the employee's duties, do not interfere with the efficient operation of City, and are not otherwise prohibited by this policy or any other City policy.
- **Accessing User Accounts:** Unauthorized attempts to access or monitor another user's electronic communications are prohibited. Unauthorized accessing, reading, copying, changing, disclosing, or deleting another user's messages, files or software without permission of the owner is prohibited.
- **Backup Copies.** All data on the Computer System is subject to backup at the discretion of the City.
- **Deleting Electronic Communications.** Users of the Computer System should be aware that Electronic Communications are not necessarily erased from the Computer System when the user "deletes" the file or message. Deleting an Electronic Communication causes the Computer System only to "forget" where the message or file is stored on the Computer System. In addition, Electronic Communications may continue to be stored on a backup copy long after it is "deleted" by the user. As a result, deleted messages often can be retrieved or recovered after they have been deleted.
- **Criminal Laws.** Under C.R.S. Section 18-5.5-101 et seq., criminal sanctions are imposed for offenses involving computers, computer systems, and computer networks. Any person committing an offense with respect to them may be subject personally to criminal sanctions and other liability. Federal laws may also apply to some circumstances.
- **Copyright Infringement.** The Copyright Laws of the United States prohibit unauthorized copying. Violators may be subject to criminal prosecution and/or be liable for monetary damages.

In general, you may not copy, download, install or use software on the Computer System without acquiring a license from the publisher. (For example, you may not copy it from a friend or other source.) Furthermore, you may not copy City's software, unless such copying is specifically authorized by the City and permitted by the license agreement.

The ability to download documents from the Internet, and to attach files to E-mail messages, increases the opportunity for and risk of copyright infringement. A user can be liable for the unauthorized copying and distribution of copyrighted material through the use of download programs and E-mail. Accordingly, you may not copy and/or distribute any materials of a third party (including software, database files, documentation, articles, graphics files, audio or video files) unless you have the written permission of the copyright holder to do so. Any legal questions regarding copying or downloading should be directed to the City Attorney; any technical questions should be directed to the IT Department.