CITY OF THORNTON
Office of the City Manager

ADMINISTRATIVE DIRECTIVE 2-36
May 29, 2008

USE OF ELECTRONIC MAIL AND COMPUTER FILES

1.0 Purpose:

To establish the City's policy regarding access to and disclosure of electronic mail messages ("email") and other computer files created, sent or received by City of Thornton employees through the use of the Internet, the City's electronic mail system, or saved on a City data storage device.

2.0 Scope:

This Directive applies to all City employees and agents of the City who utilize the City's email and/or computer systems.

3.0 Definitions:

3.1 "Electronic snooping" is defined as:

a) The unauthorized use of or attempt to use another employee's password.

b) The unauthorized entry to or attempt to enter the computer files and communications of another.

c) The unauthorized entry or attempt to enter the encrypted storage of email messages.

3.2 "Electronic tampering" is defined as:

a) The unauthorized interference with or changing of another employee's password, computer files, email or other electronic work product.

b) The unauthorized encrypted storage of email messages.

3.3 As used herein, "email shall refer to both the City and Internet electronic mail systems and any attachments to the email message. Computer files shall refer to any file, record, document, database or image stored on a City of Thornton data storage device (e.g., a hard disk, whether attached to the employee's assigned computer (PC) or a network server).

4.0 Policy:

4.1 Information as an Organizational Asset

Email records and computer files kept in the course of conducting City business, whether on paper or computerized, may be considered public records that are subject to the disclosure requirements of the Colorado Open Records Act. Furthermore, email and computer files may be discoverable in litigation, including any personal and/or City-related information stored on an employee's personal mobile device which has been configured to send and/or receive City email.

a) Employees should have no expectation of privacy in either sending or receiving information via email or in the storage and retention of computer files.

b) All computer files, including email, are the property of the City of Thornton regardless of their physical location or the form in which they are maintained.

c) The use of email and the storage of computer files shall comply with all of the requirements set forth herein and all other City Administrative Directives and City Code.

4.2 Access to Email or Computer Files

The City reserves the sole and exclusive right to access and to disclose any email messages or computer files sent, received, created, or stored by employees.

a) When deemed necessary and authorized in writing by the City Manager or designee, Department Heads have access to all email files, communications, and computer files of an employee or former employee.

b) There is no right to privacy in email messages sent or received by employees and employees are advised of the following: messages they prepare could be forwarded by the recipient to others without the knowledge of the sender; Department Heads and supervisors may have access to messages when authorized by the City Manager or designee; and any message prepared, whether or not delivered, may be published in any form through any medium.

c) Information Technology (IT) staff authorized by the IT Director to specifically carry out their work responsibilities may access all email and computer files to correct service problems, ensure system security, retrieve or restore records or transition work when

responsible personnel are unavailable, or for other legitimate business reasons. Such access rights do not include Police Department intelligence files, internal affairs files, sex assault on child files and Internet pornographic files, unless specifically authorized by the Police Chief or City Manager.

4.3 Handling Email

a) Email, and the City computers, computer systems and networks which support it, is a public asset and is intended to be used for City business. Occasional, incidental personal use is considered consistent with the email usage policy for City employees. Examples of this use might be confirming a social engagement or sending a birthday card during the employee's break time.

b) Employees shall not send mass email messages to all employees. IT may distribute mass email messages that are directly related to the operation of the City's computer system. Any other requests for such email distribution shall be forwarded to Human Resources or the City Manager's Office for disposition.

c) Any misaddressed email shall be sent back to the original sender with a message that the email has been misaddressed and shall be immediately deleted by the receiving party. However, if the misaddressed email is in violation of this Administrative Directive or any other City policy, it shall be forwarded to the sender's Department Head and the Human Resources Manager for appropriate action.

4.4 Email and Computer System Security

a) In order to assure the security of the email and computer system, the City provides employees who have such access with password protection. Employees shall protect the City's security by changing their passwords according to published IT guidelines posted on the City's intranet.

b) Employees shall not engage in "electronic snooping or tampering" activities. Such activities may result in criminal charges in addition to disciplinary action.

4.5. Personal Mobile Devices

Employees wishing to use their personal mobile device to manage City email in lieu of a City-issued device (i.e., Blackberry) shall notify IT staff before purchasing such a device to ensure its security features are suitable for receiving and storing City data. If approved, employees will be provided and required to sign an information document from IT to ensure employees are informed of all guidelines in maintaining their personal mobile device, including, but not limited to, the following:

a) Employees are required to use the password function on their mobile device to prevent its operation until such password is entered.

b) The device must provide the capability of receiving a "kill" code message from the City's IT operation.

c) The IT Helpdesk must be notified immediately upon the loss or theft of the personal mobile device.

4.6 Retention of Email

IT does not retain email on a permanent basis. IT stores email only to the degree that allows the City to restore current email in the event of a system failure.

a) IT will establish a regular schedule for purging emails and purge emails in accordance with such schedule.

b) Employees are responsible for retaining email documents consistent with retention schedules and policies established by the City Clerk.

c) Email messages that are not listed in the City's retention schedules (e.g., announcements of meetings, routine exchanges of information or exchanges of information that have no historical value) should be deleted as soon as they have served their purpose.

4.7 Retention of H Drive and Email Contents for Former Employees

After an employee separates from the City, IT will retain the H drive and email box contents for the employee for a period of 30 days, after which the data will be permanently deleted. During this 30-day period, the supervisor of the former employee may request that the contents of these areas be made available for review, or moved to another location for long-term retention.

4.8 Email Etiquette

Employees should treat email like written memoranda, understanding that messages not appropriate for sending via written memoranda are likewise not appropriate for email.

a) In the interest of best using the storage of the email server efficiently and effectively, the following policies are set forth:

1) The use of stationery as a background for email is prohibited.

2) Whenever possible, add a link or file path to the email as an alternative to attaching documents that are available on the network.

3) Avoid the use of embedded images, clip art or other graphics in the body of an email message.

b) The following uses of email are prohibited:

1) To create, send, forward, or copy non-work related offensive, harassing, discriminatory, sexually explicit or disruptive messages or attachments.

2) To receive, download, or send copyrighted material, proprietary financial information, or similar materials without prior authorization.

3) To send or receive emails pertaining to outside employment or a business in which the employee is engaged.

4) To solicit or promote commercial ventures, or religious or political causes.

5) To send or receive emails for other non-City matters except as provided for in Subsection 4.3(a).

6) To violate any law or criminal statute.

5.0 Distribution:

5.1 All City of Thornton employees.

Signed by Jack Ethredge on: 5/29/08

Jack Ethredge, City Manager Date