CITY OF CARROLLTON

ADMINISTRATIVE DIRECTIVES

SECTION: Standards of Conduct
REFERENCE NUMBER: 1.9.15
CATEGORY: Technology
EFFECTIVE DATE: 06/26/95
TOPIC: Technology Usage
REVISION DATE/NO:
APPROVED BY:

I. APPLICABILITY/SCOPE

This directive applies to all employees who use or operate City of Carrollton technology resources. The purpose of the directive is to ensure consistency in the use of technology resources throughout the City organization, and to ensure that all information technology systems and information are safe and secure. Consistency and security in use will ensure the quality of electronic communications, enhance the efficiency of workflow, prevent copyright infringements, and support operational sustainability by reducing costs. This directive does not address or replace any other City policies or directives related to Records Retention, HIPAA, confidentiality or privacy.

II. DEFINITIONS

Technology Resources: Includes computers, computer equipment, and computer accounts provided by the City of Carrollton, information resources, electronic communication facilities (including electronic mail, telephone mail, Internet access, network access, mobile phones, PDAs, fax machines) or systems with similar functions used by the City of Carrollton, regardless of ownership.

Confidential Information: Information maintained by the City of Carrollton that is exempt from disclosure under the provisions of the Texas Open Records Act or other state or federal law, attorney work product, attorney client privileged and law enforcement communications

IT Steering Committee: This IT Governance group is composed of the City Manager and other senior managers. They meet periodically to discuss current and strategic needs of the City of Carrollton. In cooperation with the IT Department, the Executive Team functions to determine city-wide standards and policies related to electronic Technology.

Messaging: Technology used to send any kind of electronic messages between network users. This currently includes Email (using Outlook or other web-based mail clients), voice-mail and Instant Messaging.

Network: A group of computers and peripherals that share information electronically typically connected to each other by either cable, wireless or microwave link.

Peripherals: Special purpose devices attached to a computer or computer network, such as printers, scanners, plotters and similar equipment.

Server: A computer that contains information shared by other computers on a network.

User: Any individual who uses, logs in, attempts to use, or attempts to log in to a system, whether by direct connection or across one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software or both.

Logon Account: A set of credentials, which includes a username and its associated passphrase, used to access technology resources, and which uniquely identifies the person attempting such access. There are many different technology resources which require specific logon accounts.

Passphrase: Series of characters, either alphanumeric or special, which are used to gain authorization to access the City network. The intent is to get away from single, simple words that are easy to guess.

Primary Network Logon Account: The account used by all employees to log into their PCs, laptops, Email and file servers. Employees must log into this account before any access to technology resources is granted.

III. ACCEPTABLE USE

A. City of Carrollton technology resources are provided for business use.

B. Use of Technology Resources and the Internet is a privilege, not a right. Department heads shall be responsible for the identification of both appropriate and inappropriate use.

C. The City of Carrollton reserves the right to suspend access to technology resources at any time, without notice, for technical reasons, possible violation, security or other concerns.

D. Technology Resources and Internet access are provided as tools for our organization’s business. The City of Carrollton reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, any and all usage of the Network and the Internet, as well as any and all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this usage. All such information, content and files are the property of the City of Carrollton. An employee should have no expectation of privacy regarding them.

E. All Internet activity is logged. Employees must not attempt to bypass Internet usage logging mechanisms.
F. Employees shall be prohibited from using the City of Carrollton technology resources for the following activities:

1. Downloading software without the prior authorization of the City of Carrollton IT department.

2. Printing or distributing copyrighted materials, or using such materials in a manner that is in violation of any licensing agreements. This includes but is not limited to, software, articles and graphics protected by copyright and licensing laws. Only the City's IT Department is authorized to duplicate, transfer or lend licensed software or related documentation authorized by the City, but may do so only in accordance with copyright protection laws and guidelines.

3. Sending, printing or otherwise disseminating City of Carrollton confidential data or any other information deemed confidential by the City of Carrollton, to unauthorized persons. Employees must comply with any other city, state or federal regulations with regards to sensitive or personal information.

4. Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of employment

5. Making offensive or harassing statements based on race, color, religion, national origin, veteran status, ancestry, disability, age, sex or sexual orientation

6. Sending, soliciting or forwarding messages containing defamatory, obscene, offensive, sexually oriented or harassing statements or images. An employee should notify their supervisor and/or Workforce Services Manager immediately upon receiving such a message. This type of message should not be forwarded.

7. Attempting to circumvent technology used to prevent access to content that has been deemed inappropriate to the workplace.

8. Engaging in any other criminal activity in violation of local, state or federal law.

9. Intentionally introducing a virus, harmful or malicious component, or corrupted data to any City of Carrollton computer systems.

G. All employees must refrain from storing information relating to their job function on their local hard drives. Instead, employees must save such data in a folder on a network server which is properly secured and is being backed up on a regular basis. Each employee and department is assigned space on the network file server for this purpose.

H. Any unauthorized software, files or hardware found on a computer during an audit will be brought to the attention of the appropriate level of supervision for resolution and may result in the removal of the unauthorized software or hardware and disciplinary action.

I. City employees may only use software or technical resources approved or provided by the City. The software must be installed by the IT department.

J. If an employee requires the regular use of an approved software product at home, he or she shall contact the IT Department to obtain a valid license for such software. All software must be uninstalled upon cessation of its use at home or termination of employment.

IV. <u>SECURITY</u>

A. Each employee who is authorized to access technology resources is responsible for the actions associated with their logon accounts. All employees must take the appropriate measures to ensure that unauthorized persons do not access the City network with their logon accounts.

B. Personal Passphrase Practices

1. Each employee with approved access to city technology resources is responsible for creating original, unique and strong passphrases (something known only to them and not easily guessed) for each logon account.

2. Each passphrase owner must safeguard and protect each passphrase they have created, or that is entrusted to them.

3. Passphrase sharing is strictly prohibited. Sharing of workstations and software must be accomplished without sharing passphrases. [*Please consult with the IT Department as necessary.*] There may be cases where technical troubleshooting is necessary for a personal profile. In this situation, a technician may need to mimic an employee by creating a temporary randomly generated passphrase for the account and then setting the account to have its passphrase reset upon next logon. Under no circumstances will the IT department ever ask an employee for their passphrase. City employees must never divulge their passphrase to anyone, including their supervisor.

4. Writing down passphrases is not an acceptable practice; however, if passphrases must be stored, the information shall be stored securely and be accessible only by the employee who is responsible for the account. Input of passphrases via electronic file or programmable function keys, scripts, macros or automated logon sequences is strictly prohibited.

5. The IT Department is directed to establish and configure network systems to adhere to the following standards and mechanisms for establishing, maintaining and changing passphrases:

- Passphrases should be at least eight (8) characters, should expire every sixty (60) days, should not be the same as any of the previous six (6) passphrases, and should be complex.

- Passphrase complexity is defined as using at least three (3) of the following types of characters: upper case letter, lower case letters, numbers and special characters.

- To prevent brute force attacks against the network, primary network logon accounts will be temporarily locked out after three (3) failed logon attempts within a specified amount of time.

- The accounts will automatically unlock fifteen (15) minutes after being locked out.

6. When creating a new passphrase for their primary network logon, employees must follow the standard listed above. For example, by making sentences separated by special characters, it is much easier to create a long passphrase which can be remembered without having to write it down. Dictionary words must not be included in a user’s passphrase unless the user is implementing the sentence approach. The user’s name or the names

of family members must also be avoided. The following examples would be considered strong passphrases that are easy to remember:

- "Under-the-rainbow"
- "Changed_my_tire"
- "Deliver*the*mail"

7. This standard must be used for all other logon account passphrases where supported by the application. For example, an application might only allow six (6) characters, or might not allow special characters. In these cases, users must adhere to the standard as much as the application will allow.

8. The City will be deploying a Single-Sign-on solution, which allows users to access the majority of their applications by logging into their primary network logon. This technology, when in use, will allow employees to utilize a self-service portal to reset their own passphrases. If an employee cannot remember their passphrase, and is unable to reset it using this tool, they must personally appear at the IT help desk so that their identity can be verified prior to resetting the passphrase. This is to ensure that nobody else can impersonate that employee in order to gain access to their account. If the employee does not have the ability to make a personal appearance at the help desk, they must contact their supervisor and have them appear at the help desk to verify their identity. The help desk can then call the employee back and present them with their temporary passphrase.

C. Shared Logon Accounts

1. All logon accounts must uniquely identify the person using the account. Use of shared logon accounts is strictly prohibited unless approved in advance by the City's IT Steering Committee. A valid business reason must exist in order to justify the use of such accounts.

2. In situations where shared logon accounts have been granted proper approval, the employees using these accounts must keep the passphrases associated with these logon accounts confidential and must refrain from disclosing the passphrases to anyone else.

D. Additional Security Responsibilities

1. All city computing devices are to be equipped by the IT Department with security mechanisms to protect the information and resources of each system. Employees must not tamper with, reconfigure, or disable such mechanisms. Such mechanisms would include, but not be limited to anti-virus software, spyware protection and access policies

2. All employees are required to safeguard computer devices entrusted to their care. Unattended devices which have open network access create significant security vulnerabilities. Employees must lock or log off of their workstations, laptops or handhelds whenever they are left unattended for any period of time. The IT department will deploy a password-protected screensaver on PCs and laptops which will be activated after ten (10) minutes of no user activity as a safeguard. Employees are expected to implement similar safeguards on their handheld devices whenever technically feasible.

3. All remote connections to the City's network using handheld devices must be through the use of the Blackberry Enterprise Server. Any existing devices that use other methods prior to this policy going into effect , such as Windows or Apple systems, will be grandfathered for the life of the current device or for a maximum of two years, whichever comes first. The IT department may provide additional options for connection as new technical solutions surface in the future.

4. City technology resources must not be used to obtain illegal access to computer systems, to interfere with the normal operations of computer systems or to perform malicious acts against a computer system

5. City employees must never test the security of computer systems, whether physical or logic based. The only exception to this is if such security testing is a known part of the employee's job description and function.

E. Auditing

1. The IT Department will periodically conduct random audits of all technology resources. During any of these audits, the IT Department will search for and remove computer viruses and unauthorized software, files and hardware.

V. SUSTAINABILITY OF SOFTWARE AND HARDWARE

A. Development of Software/Work Products

1. In order to achieve its goal of sustainability, the City has adopted an approach towards software and applications that favors Enterprise-wide standardization over custom-built applications. The enterprise approach, using Commercially Available Off the Shelf (COTS) products, is more sustainable throughout the life of the application. Commercially available PC software products shall be used when available. When such products are not available, departments must contact the IT Department to see if there are any feasible alternatives.

2. All software and work products (documents, databases, spreadsheets, etc.) developed for City projects by persons covered under this policy on City time utilizing City owned computer systems remain the property of the City. Such software or work products are for the exclusive use of the City or City contractors.

B. Budgeting

1. The total costs of computer hardware, software acquisition, wiring, training, support, and ongoing maintenance should be included when preparing cost estimates for budgeting to ensure the entire package is considered for budget planning purposes.

2. The City of Carrollton's established purchasing procedures must be followed in coordination with the IT Department.

3. Department Directors will coordinate with the IT Department via the help desk for the implementation of all computer hardware, software, networking equipment, printers, and other peripherals and devices for the City of Carrollton. A service request should be submitted to the IT Department and should be completed with the appropriate charge codes in order for IT Department to complete the purchase.

C. Approved Software

1. The IT Department must be contacted prior to purchase or installation of software products for the purpose of technical support and compatibility. The following criteria will be used in evaluating new software systems:

a) Compatibility with existing hardware and software, including security systems

b) Ability/Inability to achieve same purpose with an existing product

D. Upgrading PC Hardware/Software

1. PC hardware and software upgrade requests shall be made by following the purchasing procedure described above. The IT Department shall carefully review these requests in light of current City practices and business objectives.

E. Installation/Downloading

1. All installations/downloading of PC software shall be managed by the IT Department including those contracted with a third party.

2. Once the software is installed on a hard drive, original media shall be kept in a safe storage area maintained by the IT Department.

3. Employee installation and downloading of any programs from the Internet, such as screensavers, utilities, beta software, instant messaging and file sharing applications, internet-based games and shareware is strictly prohibited.