INFORMATION TECHNOLOGY MANUAL

CITY OF SOCORRO, TEXAS. INFORMATION TECHNOLOGY POLICY

1. PURPOSE

It is the purpose of this policy to establish ethical guidelines for the use of the City's IT assets and computing facilities.

(IT assets include component hardware and software and these entail servers, laptops, iPads, tablets, workstations, switches, routers, firewalls, bridges, printers, fax machines and photocopiers, cell phones, e-mail, Internet, modems, firewalls, operating systems, applications software, business applications, city's data and information).

2. SCOPE

The scope of the policy is for broad City usage and it applies to the City's contingent workforce (all employees) as well as non-City hardware/software contractors, vendors, suppliers and any stakeholders that provide services to the City and that bring themselves into contact with the City Information Technology (IT) infrastructure.

3. PRINCIPLES

The City encourages the use of IT facilities to make work processes more efficient and effective. The guidelines shall attempt to provide a workplace in which employees are allowed to succeed in a highly productive environment and where high standard of morality, ethics, fairness and integrity exist.

Adherence to these guidelines by all City's employees protect the right of all workers with regards to privacy and freedom of expression, and guarantees that the City operates in a manner consistent with legal and ethical practices.

The City's IT assets, infrastructure and equipment remain the property of the City at all times. The City provides these facilities in order to improve the productivity of employees in the course of executing their job functions.

The City's IT facilities are intended for business purposes only and not for private/personal work. The access to and use of City's IT facilities is a privilege and not a right. Every employee has a responsibility to maintain and enhance the City's public image and to use the City's IT facilities in a productive manner.

4. ROLE OF THE INFORMATION TECHNOLOGY (IT} Department

4.1.1 Provide new employees with access to a desktop or laptop account, and access to an email account, and work cell phone if required by job description; **once the employee has cleared the background check by Human Resources.**

4.1.2 Employees who receive a work cellphone, iPad or Tablets shall sign a device policy form.

4.1.3 New employees will be given temporary passwords for desktop and email accounts, and it is their responsibility to change it and secure it.

4.1.4 No new computers, printers, and/or any computer equipment shall be bought without approval and authorization from the IT Department.

4.1.5 No software packages are to be purchased and installed without the approval and authorization from the IT Department.

4.1.6 The IT Department **MUST ALWAYS** be notified of all computer faults before anyone or any service provider from outside is called to fix the problem or any computer equipment which is being moved from one location to another.

4.1.7 It is the employee responsibility to submit an IT work order request for any issues stated above.

5. ACCEPTABLE USE POLICY - DESKTOPS AND LAPTOPS

This po/icy defines end-user acceptable use of City's IT equipment. The policy applies to desktops, laptops, tablets, printers, and other equipment provided by the City. Anyone that uses City's equipment including employees, vendors, contractors, and visitors, must adhere to this policy. Acceptable use applies to proper care, handling and maintenance of equipment as well as following documented security policies relating to equipment use.

5.1 User Responsibilities

Users shall use City provided IT equipment responsibly and for City business purposes only. Appropriate use policies are:

5.1.1 Active desktops and laptops may not be left unattended for prolonged periods of time. Users should secure their workstation when leaving the workstation unattended.

5.1.2 City's information displayed on screens or on reports shall be treated as confidential and private. Users must guard municipal information from unauthorized access or use.

5.1.3 Any employee-signed confidentiality agreement shall fully apply to information accessed with City IT equipment.

5.1.4 Director, Managers and Supervisors are responsible to ensure that their employees are adequately trained on appropriate use of IT equipment with in their department, and that they adhere to this policy.

5.1.5 Users may not grant access to non-employees, including vendors or contractors, without approval of their Director or approval by the IT Depańment.

5.1.6 Users shall keep their equipment clean and free from dust. Users shall maintain "breathing space" around equipment in accordance with equipment installation instructions.

5.1.7 Users shall not eat or drink at their workstation.

5.1.8 Desktop acceptable use policies apply equally to portable devices, including laptops, notebooks, and iPad, tablets, and cell phones.

5.1.9 All acceptable use polices apply equally to non-City provided equipment if the equipment accesses City's information or networks.

5.1.10 Users who access City's information and computer systems from remote locations must adhere to this policy.

5.1.11 City's provided equipment shall be kept in a secure manner so that the employee's household members and others do not have access to the device when not in the office.

5.1.12 **Users should not store City' information or files locally only. The use of shared or network drives for all municipal information is required.**

5.1.13 Users are responsible for backing up files stored on their desktop or laptop. The IT department will not provide backups at the desktop level.

5.2 Prohibited practices

Any activity, action, or lack of action on the part of a user that damages the City or compromises security or confidentiality is prohibited. Examples of prohibited practices include:

5.2.1 Installing new desktops or equipment without prior approval by the IT Department.

5.2.2 Upgrading equipment or adding peripheral equipment without prior approval of the IT Department.

5.2.3 Downloading and/or installing programs that are not specifically approved by the IT Department.

5.2.4 Using unlicensed software. Users may not copy and share software that is installed on their desktops or laptops with other users. Using programs or Internet web sites that compromise the privacy of customers or employees.

5.2.5 Removing or compromising desktop virus protection programs.

5.2.6 Opening email attachments that are inappropriate or from someone you do notknow.

5.2.7 Using City's provided IT equipment for non-business reasons or for personal gain.

5.2.8 Unauthorized attempts to break into any workstation.

5.2.9 Unauthorized access to City files, programs, databases, or confidential information.

5.2.10 Sending or posting confidential files to unauthorized persons.

5.2.11 Failing to fully cooperate with IT security investigations.

5.2.12 Allowing co-workers or other users to use your desktop without approval of your Director or by the IT Department.

5.2.13 Sharing password information or displaying it in plain view on or around your desktop. Users must secure their passwords and not reveal them to others.

6. ACCEPTABLE USE POLICY- EMAIL

This policy defines end-user acceptable use of City provided email services. This policy applies equally to on-site usage as well as remote usage of City email. When using City email, users shall follow these guidelines:

6.1 User Responsibilities

6.1.1 E-mail users shall use e-mail in accordance with general communications policies of the City.

6.1.2 City provided e-mail generally shall be used for business communications only.

6.1.3 Users understand and agree that they shall not have a right to privacy when using City e-mail or electronic communications, even if those communications are of a personal nature.

6.1.4 **Departmental heads and/or the Human Resources Department should immediately advise the IT Department of any resignations so that their-mail and business application access credentials are disabled (terminated) for security reasons.**

6.2 Prohibited Practices

6.2.1 Users should not open e-mails or e-mail attachments from persons unknown to them. Opening of unknown or suspicious attachments can have serious consequences for the City in terms of viruses or computer worms. Users should contact the IT Department if there is even a slight concern about an e-mail attachment.

6.2.2 Users should not respond to spam e-mailsor unsolicited advertisements, responding will multiply the amount of spam received. Unsolicited e-mails should be deleted or reported to the IT Department.

6.2.3 Users may not use e-mail to solicit employees for any purpose, including charitable purposes, without the written approval of their department Director.

6.2A Users may not forward or promote spam or joke e-mails, and particularly may not send spam or joke e-mails to group e-mail addresses.

6.2.5 Users should not access, create, display, download, save or transmit threatening, racist, sexist, obscene, offensive, annoying or harassing language and/or materials such as broadcasting unsolicited messages or sending unwanted mail.

6.2.6 Users may not use e-mail for purposes that violate legal or City policies regarding gambling, hate, pornography, or other inappropriate purposes.

7. ACCEPTABLE USE POLICY - INTERNET

This policy defines end-user acceptable use of City provided Internet access. This policy applies equally to non-City provided Internet access made while on City premises.

When using Internet, users shall follow these guidelines:

7.1 User Responsibilities

7.1.1 City provided Internet access generally shall be used for business purposes only. Users may not use Internet for personal reasons.

7.1.2 The IT Department shall be responsible for installing and updating anti-virus software on all computers. IT will be responsible for weekly or monthly desktop scanning which is normally required to eradicate spyware and latent viruses.

7.1.3 Users understand and agree that they shall not have a right to privacy when using Internet on City provided equipment.

7.1.4 Users understand and agree that the City may severely limit access, including the use of controls that prevent access to sites deemed inappropriate by the City. The City has the right to monitor and control Internet usage at its sole discretion.

7.1.5 Users agree that the City will decide which websites can be accessed using the guidelines provided by the service provider. This will be monitored on an ongoing basis and amended from time to time as required.

7.1.6 Website can automatically be blocked by the service provider if the site is exposed from a security perspective or if the site is used for inappropriate purposes.

7.2 Prohibited Practices

When using Internet, users must follow these guidelines:

7.2.1 Users should not download software or images unless they are from a trusted source, and then only if authorized by the IT Department. Opening of unknown or suspicious programs or images can have serious consequences for the City in terms of viruses or computer worms. Users should contact the IT Department before they download any files from the Internet.

1.2.2 Users should not provide their e-mail address when registering at a website unless the web site has a clear policy that they will protect e-mail privacy.

7.2.3 **Users should not use the Internet for on-line radio or television access without permission from the IT department. Sites that provide streaming content have a significant impact on network resources and impact network performance and responsiveness.**

7.2.4 Users may not use Internet for purposes that violate legal or City policies regarding gambling, hate, pornography, or other inappropriate purposes.

7.2.5 Users shall not access, create, display, download, save or transmit any text, file picture, graphic or sound clip or engage in any conference that includes material which is obscene, libelous, indecent, vulgar, profane, and lewd or which advertises any product or service not permitted to minors by law.

7.2.6 Users shall not engage in activities that damage hardware or software, disrupt communication, waste systems resources, or overload Networks with excessive data.

7.2.7 Users shall not access chat rooms to carry out non-business related matters.

8. ACCEPTABLE USE POLICY - BUSINESS APPLICATIONS

This policy defines end-user acceptable use of City's business application software. This policy applies to all software identified by the City as a business application. General Accounting and Financial Management software, Court, and IT programs are examples of business applications. Anyone that uses City's business applications including employees, vendors, contractors, and visitors, must adhere to this policy.

8.1 User Responsibilities

Users shall use City provided application software responsibly and for City business purposes only. Appropriate use policies are:

8.1.1 All IT Infrastructure Acceptable Use Policies fully apply to application software usage. This includes the requirement that active desktops and laptops may not be left unattended for prolonged periods of time. Users should secure their workstation when leaving the workstatíon unattended.

8.1.2 City information display on equipment or on reports shall be treated as confídential and private. Users must guard Cíty ínformation from unauthorized access or use.

8.1.3 Directors are responsible to ensure that their employees are adequately trained/educated on appropriate use of City software applications within their department, and that they adhere to this policy.

8.1.4 Directors are responsible to assure that users have adequate access to applications, but do not have access that is inappropriate for their job function or otherwise represents an unnecessary security risk for the City.

8.1.5 Users may not grant access to non-employees, including vendors or contactors, without approval of their Director or IT Department.

8.1.6 Users who access City informatíon and computer systems from remote locations must adhere to this policy.

8.1.7 Users should promptly report software problems or apparent defects to their Directors. Directors should work with the IT Department to determine if the issue is software related, and if so, how is best to have it fixed.

8.2 Prohibited Practices

Any activity, action, or lack of action on the part of a user that damages the City or compromises security or confidentiality is prohibited. Examples of prohibited practices include:

8.2.1 Installing new software applications without prior approval by the IT Department. This includes downloading software from the Internet, even if there is no charge for the software.

8.2.2 Downloading applications for evaluation purposes is also prohibited unless approved in advance by the IT Department.

8.2.3 Sharing passwords with other users. Users shall not post or display their passwords where they can be seen by others.

8.2.4 Attempting to access applications without approval. Employees shall not attempt to gain access or hack into an application that they are not authorized to access.

8.2.5 Using unlicensed software. Users may not copy and share software that is installed on their desktops or laptops with other users.

8.2.6 Using programs or Internet web sites that compromise the privacy of customers, or employees.

8.2.7 Unauthorized access to City files, programs, databases, or confidential information.

8.2.8 Sending or posting confidential files to unauthorized persons.

8.2.9 Failing to fully cooperate with IT security investigations.

9. COMPLIANCE

Management in conjunction with the IT Department of the City may deem it necessary to search any computer drive or file system for alleged violation of this policy. Violations will be noted and reported.

The City retains the right to randomly monitor and intercept all Employee communication, regardless of whether they are of a business or personal nature, including but not limited to e-mail and Internet usage. Whenever an IT administrator is on-site at a branch or any satellite location, he or should test at random, compliance levels at the individual desktop level.

The monitoring of communications on the City IT infrastructure is not a "witch-hunting" exercise. It is necessary for the support and maintenance of this valuable infrastructure. Users should report inappropriate e-mails, usage, handling or any policy violations to the IT Department immediately.

Note: Any Employee who abuses the privilege of City facilitated access to IT will be subject to corrective action.

Any action (on IT facilities, computer equipment, business applications, e-mail or the Internet) that may expose the City to risks of unauthorized access to data, disclosure of information, illegal liability, or potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

If necessary, the City also reserves the right to advise appropriate legal officials of any illegal violations. Employees that violate this policy will be disciplined and may be dismissed/terminated for serious or multiple violations.

10. COMMUNICATING THE IT POLICY

Copies of the IT policy shall be provided to all Departments Heads who will then review the policy with all employees in their respective departments.

10.1 Each employee of the City shall sign and date the acceptance form, and shall return the form to the Human Resources Department for retention in employee records.

10.2 The final draft of this policy shall be included within the City's "handbook" of company's policies, and shall be presented to all newly hired employees at the start of their employment.

10.3 Acceptance of the IT Policy by a new employee shall be denoted by signing and dating the acceptance form and returning the form to the Human Resources department for retention in employee records.

10.4 The City employee, who contracts for services provided by software contractors, or vendors/suppliers providing services to the City, is responsible for providing the contractor/vendor/supplier with a copy of these policies before any access to Company IT/ facilities/assets is granted.

11. AMENDING THE IT POLICY

11.1 The City reserves the right to amend these policies and practices at any time without prior notice and to take such further actions as may be necessary or appropriate to ensure compliance.

11.2 The City's IT Policy shall be reviewed annually to comply with applicable state, local government laws, regulations and policies that govern the workplace.

11.3 Amendments to the IT Policy shall be reviewed and approved by City Manager and City Council.

11.4 The amended draft of the policy shall be legally reviewed and approved before the amended policy is considered to be a City policy.

11.5 The City shall publish the amended IT Usage Policy in the workplace to ensure that all employees are notified of the amendments to the policy.

11.6 Copies of the newly amended policy shall be given to all Heads of Departments of the City who will then review the policy with all employees from their respective departments.

11.1 Sign-off of the pre-existing IT Policy by a current employee of the City shall constitute acceptance of the newly modified version.

11.s All personnel employed by the City subsequent to the IT Policy amendment(s), shall be required to sign the acceptance sheet to the terms of this newly amended City policy.

11.9 The City employee who contracts for services provided by software contractors, or vendors/suppliers providing services to the City is responsible for providing the contractor/vendor/supplier with a copy of the amended policies before any further access to IT assets is granted.

Approved by City Council _9/17/2015_:

Jesus Ruiz, Mayor