ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology
Effective Date: December 1, 2005
Revision Date(s):

I. PURPOSE:

The purpose of this Administrative Directive (AD) is to provide guidance regarding the acceptable use of computer equipment, networks and other information technology hardware and software in the City of San Antonio ("City").

II. POLICY

A. The City provides access to its technology systems to assist technology users in performing their duties efficiently and effectively. Inappropriate use of information technology exposes the City to internal and external risks and may reduce the effectiveness of those systems. All users of City-owned and managed information technology are responsible for using that technology in an appropriate and lawful manner. Any activity performed on a workstation under an employee's login ID is presumed to be performed by that employee.

B. There should be no expectation of privacy in the use of City-administered technology or equipment. Due to the City's need to protect resources and assets, and its obligation to comply with Texas Public Information Act (Chapter 552, Texas Government Code) open records requirements, there is no expectation of confidentiality of information maintained on any storage or network device belonging to the City unless it is specifically protected by law from disclosure and then only to the extent of that legal protection.

C. All information generated by or stored on city-provided equipment is the property of the City of San Antonio. There should be no expectation of confidentiality with regard to any files, including email, stored on any City-managed computer.

D. Technology users shall use City-managed technology for official business, but may make and receive personal communications, including telephone calls during business hours, that are necessary and in the interest of the City. While some incidental use (as defined below) of City-managed technology is unavoidable, such incidental use is not a right, and should never interfere with the performance of duties or service to the public.

E. This Directive will support existing and forthcoming technology-related Directives, and will apply to all users of the City's information technology and networks unless otherwise specified in this document.

III. DEFINITIONS:

A. City: The City of San Antonio, its departments and agencies.

B. City-administered technology or equipment: Any technology or equipment that is used and/or managed by the City even if the City does not own said technology or equipment. City-managed technology includes technology or equipment owned by the City, on loan to the City, funded by grants, leased by the City, etc. Technology includes, but is not limited to, computers, mobile communication devices, telecommunication devices, servers, networks, software, databases and e-mail messages.

C. DSS: The person who is filling the role of technical specialist for a department. This role is typically called a Department Systems Specialist (DSS) or Department Systems Manager (DSM).

D. E-mail spoofing: Forging an e-mail header to make it appear as if it came from someone other than the actual source.

E. Federal statutes: The laws of the United States and/or the country where the user is located.

F. Incidental personal use: Any personal use of City-owned or managed technology that:

a) does not cause any additional expense to the City;

b) is infrequent and brief;

c) does not have a negative impact on overall employee productivity;

d) does not interfere with the normal operations of an employee's department or work unit;

e) does not compromise the City in any way;

f) does not embarrass either the City or the employee;

g) does not contravene other elements of this policy; and

h) serves the interests of the City in allowing employees to address important personal matters which cannot be addressed outside of work hours without leaving the workplace.

Examples of personal communications that could be in the interest of the City include:

a) communications to alert household members about working late or other schedule changes;

b) communications to make alternative child care arrangements; communications with doctors, hospital staff, or day care providers;

c) communications to determine the safety of family or household members, particularly in an emergency;

d) communications to make funeral arrangements;

e) communications to reach businesses or government agencies that can only be contacted during work hours;

f) communications to arrange emergency repairs to vehicles or residences.

City departments, in consultation with the Human Resources Department, may determine whether a use is personal or business and if usage is personal, whether it is incidental.

G. ITSD: the City's Information Technology Services Department or successor agencies.

H. Local statutes: The ordinances, statutes, and laws of the City, Bexar County and/or the municipality or county where the user is located.

I. Malware: Short for **mal**icious soft**ware**, software designed specifically to damage or disrupt a system, such as a virus, worm, Trojan horse, or e-mail bomb.

J. Network: A group of two or more computer systems linked together to facilitate communication, data sharing and processing among the systems.

K. Phishing: The act of sending an e-mail falsely claiming to be an established legitimate enterprise in an attempt to manipulate someone into surrendering private information that can be used for identity theft or other malicious purposes. The e-mail directs the receiver to a web site that appears to be owned by the legitimate enterprise and asks for private information to be used in identity theft or other malicious purpose.

L. Public access terminals: Computers provided by City for use by the general public.

M. Spam (called "unsolicited commercial electron mail messages" as it is defined by the State of Texas statutes): A commercial electronic mail message sent without the consent of the recipient by a person with whom the recipient does not have an established business relationship. The term does not include electronic mail sent by an organization using electronic mail for the purpose of communicating exclusively with members, employees, or contractors of the organization.

N. State statutes: The statutes and laws of the state of Texas and/or the state where the user is located. Where statutes from two states conflict, the statutes of the State of Texas shall take precedence.

O. Technology user: Any employee, contractor, consultant, part-time or temporary employee who uses City-administered technology or equipment, and anyone accessing the City's networks, exclusive of the City's web pages.

IV. POLICY GUIDELINES:

This Directive applies to any party using city-owned or city-managed technology, or any party connecting to the City's networks. All equipment or technology that is owned or administered by the City is included within this AD's scope. Public access terminals provided by the City are **not** included in the scope of this policy, except where those terminals are used by City staff to access the City's networks.

RESPONSIBILITIES:

Information & Technology Services Department

A. Organizational responsibility for the development, implementation, maintenance, and compliance monitoring of requirements established in this Directive is placed with the Information & Technology Services Department (ITSD).

B. ITSD, along with the Human Resources Department, will provide City departments with initial communication and training regarding this Directive. However, Department Directors are ultimately responsible for communicating the policies and standards established in this Directive to all personnel in their respective departments

and for ensuring compliance within their respective departments with those policies and standards.

C. ITSD may disconnect any computer from the City network at any time if continued connectivity constitutes a threat to the City or City-administered technology or equipment. ITSD will attempt to contact the DSS responsible for the computer prior to disconnecting as long as such notification does not allow further degradation of the City-administered technology or equipment. Such notification will be made after the disconnection if prior coordination was not possible.

Department Directors and their designees

A. Department Directors are responsible for any disciplinary action taken against employees who violate this Directive in accordance with section VI. The Human Resources Department will provide guidance as required to City departments regarding appropriate disciplinary action to be taken against employees who violate this policy.

Office of the City Clerk

A. The Office of the City Clerk is responsible for the creation, maintenance and administration of all rules regarding the classification and protection of information stored on City-administered technology or equipment.

Employees

A. Employees are accountable for the proper use of City-owned technology, and should be aware that they are responsible for any information that they generate or distribute through the City's technology systems. Any activity performed on a workstation under an employee's login ID is presumed to be performed by that employee.

B. Employees should be aware that all information generated by or stored on city-provided equipment is the property of the City of San Antonio. There should be no expectation of confidentiality with regard to any files, including email, stored on City computers. Any materials stored on City equipment may be monitored and reviewed by City management at any time.

C. Employees should be aware that most information generated and stored on City-provided equipment is subject to applicable open records laws.

Human Resources

A. Human Resources will provide guidance to departments for disciplinary actions associated with violations of the Directive.

B. Human Resources will assist ITSD in providing training regarding this directive to current and future employees. Following implementation of this directive, Human

resources will ensure that all new employees are provided a copy of this directive and complete the attached acknowledgement.

C. The Human Resources Director will consult with the Chief Information Officer in approving any monitoring of systems for personnel reasons.

V. PROCEDURES:

A. General use and ownership of information technology

1. City-administered technology and equipment is for use in conducting City business with the exceptions noted in this Directive. Technology users should be aware that the data they create, receive, or forward on the City's systems remains the property of the City.
2. Incidental personal use (as defined in this Directive) of City-administered technology or equipment is permissible as long as it does not interfere with the performance of assigned duties, does not have a detrimental effect on City information technology and systems, and is not prohibited by this policy. Personal use should be limited to those necessary activities described in the definition of "Incidental Use" above.
3. Supervisors are responsible for monitoring the incidental personal use of information technology by their employees. If departmental management determines an employee's usage is not allowable as incidental personal use, management should notify the employee immediately. Continued unacceptable personal use by that employee shall be disciplined in accordance with section VI. If an employee is not sure usage is acceptable, he/she should consult his/her supervisor for guidance.
4. There should be no expectation of privacy in the use of City-administered technology or equipment. Because of the City's need to protect its resources and assets and its obligation to comply with Texas Public Information Act (Chapter 552, Texas Government Code) open records requirements, there should be no expectation of confidentiality of information maintained on any storage or network device belonging to the City unless it is specifically protected by law from disclosure and only then to the extent of that legal protection.
5. The City does not routinely monitor employee use of City-owned and managed technology. However, the Chief Information Officer or his/her designee may monitor City-administered technology or equipment at any time for security, network maintenance or audit purposes, with or without consent of the technology user. Monitoring of technology usage for personnel-related matters shall require the approval of the Chief Information Officer and the Human Resources Director.

B. Security and proprietary information

1. Information stored on City-administered technology or equipment should be classified in accordance with federal, state, and local statutes, ordinances, and policies regarding the confidentiality of the information as prescribed by the Office of the City Clerk. Employees should take the necessary steps or follow prescribed processes to prevent unauthorized access to confidential information. Unclassified information should not

be released to non-City entities without authorization and approval by the City Manager's Office.

2. Employees must comply with all City Directives regarding use of information technology, including forthcoming Directives related to:

    a. Electronic Communications (e-mail, voice and internet)
    b. Password Management
    c. Security
    d. Data management and Classification
    e. Monitoring
    f. Remote Access

3. All personal computers, laptops and workstations should be protected from unauthorized access when the system is unattended. The recommended method of securing the device is with a password-protected screensaver (with the automatic activation feature set to 15 minutes or less) or by manually locking the device (Ctrl-Alt-Delete for Windows 2000 or XP users). Devices that cannot be locked as described above should be secured by logging off the devices or turning them off.

4. Employees must take reasonable and necessary precautions to secure and protect portable devices. Protect portable devices in accordance with the following guidelines:

    a. Laptops and other portable devices used in an office setting should be locked in a drawer or cabinet or should be secured to the desktop with a device manufactured for that purpose.

    b. Users should retain physical contact with all portable devices in areas where the risk of theft is high such as airports and hotels.

    c. If a portable device must be left unattended in a vehicle, it should be locked in the vehicles trunk or otherwise secured and protected from plain view inside the locked vehicle.

    d. Portable devices should never be left in a vehicle, even if locked and out of sight, overnight. Reasonable precautions should be taken to protect the device when traveling, even if the travel is local.

5. ITSD regularly maintains operating systems, updates anti-virus software, and applies security patches by sending those updates during the evening hours to computers attached to the network. When an employee leaves for the day, he/she should log off from his/her computer, but should leave the computer turned on and attached to the network. Because laptops may be secured during non-business hours and may not be connected to the network when updates are sent, users should work with their DSS to ensure updates to portable devices are installed in a timely manner.

6. All technology devices used by a technology user to connect to the City's networks shall continually execute approved virus-scanning software with a current virus definition file. This includes employee-owned equipment attached to the City's

networks through remote access technologies. The City is not responsible for providing the required virus-scanning software for employee-owned computers.

C. Unacceptable use

The following activities are prohibited unless performed in the course of legitimate job responsibilities. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable use:

1. Engaging in any activity that is illegal under local, state, or federal statutes or which violates City of San Antonio policies and Administrative Directives;
2. Accessing, displaying, storing or transmitting material that is offensive in nature, including sexually explicit materials, or any text or image that can be considered threatening, racially offensive, or hate speech. This includes any images, text, files, etc. sent via email to co-workers or outside parties. **Accessing, storing, displaying, or transmitting pornographic materials using City-owned and managed technology is strictly forbidden;**
3. Any personal uses that interrupt City business, or which prevents an employee from performing his/her work. Employees should not use City e-mail accounts as their primary personal e-mail address. City systems shall not be used to chat online, "blog", or shop online;
4. Violating any copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City;
5. Unauthorized reading, deleting, copying or forwarding of electronic communications of another, or accessing electronic files of another without authorization;
6. Sending SPAM to either internal or external parties;
7. Unauthorized duplication of copyrighted material including, but not limited to, text and photographs from magazines, books or other copyrighted sources, copyrighted music and/or copyrighted movies. Copying or installing copyrighted software for which the City or the end user does not have an active license is not permitted;
8. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws;
9. Maliciously introducing malware or similar programs into the network or server;
10. Revealing a City account password to others or allowing use of a City account by others. This includes household members and visitors when work is being done at home. Revealing a City account password to an authorized technician during troubleshooting procedures is not a violation of this policy. In such a situation, a new password should be established as soon as possible after the problem is resolved;

11. Making fraudulent offers of products, items, or services originating from any City account
12. Using City-owned technology for political activity, private gain, gambling, shopping, games or other entertainment, or any other non-business function unless permitted by this Directive;
13. Causing security breaches or disruptions of City communications. Security breaches include, but are not limited to:
    a. Accessing data which the employee is not authorized to access or logging into a server or user account that the employee is not expressly authorized to access;
    b. Causing network disruptions for malicious purposes including, but not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
    c. Port scanning or security scanning for malicious purposes is prohibited. Non-malicious scanning that is part of a City-sanctioned security process is allowed. ITSD should be notified prior to any such scanning;
    d. Circumventing user authentication or security of any device, network or account;
    e. Maliciously interfering with or denying service through denial of service attack, or other means;
    f. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, another user's device or session, via any means, locally or via the City's network;
    g. Adding/removing hardware components, attaching external devices, or making configuration changes to information technology devices without approval by ITSD.

VI. DISCIPLINE (if applicable):

A. Failure to comply with this Directive will result in disciplinary action in accordance with the Municipal Civil Service Rules of the City of San Antonio, Rule XVII, Section 2. Discipline will be evaluated and based upon the number of violations and severity of the incident. The Human Resources Department must be consulted by a department when assessing the appropriate level of disciplinary action.

B. Employees who fail to follow and administer this Directive will be disciplined under the authority of the Department Director.

C. This Administrative Directive does not supersede the Department Director's authority over the determination of final disciplinary actions taken, particularly in cases where the safety of the general public or City employees are significantly compromised by an infraction of this administrative Directive. A Department Director may choose to assess more severe disciplinary action against an employee depending on the severity of the infraction.

ADMINISTRATIVE DIRECTIVE 7.5 Acceptable Use of Information Technology
Effective Date: December 1, 2005
Revision Date(s):

This Directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the ITSD Department at 207-8301.

Hugh Miller, Jr., Interim Director ITSD — Date: 11/15/05

Approved by:

Michael Armstrong, Chief Information Officer — Date: 11-15-05

Approved by:

Sheryl Sculley, City Manager — Date: 11-15-05

CITY OF SAN ANTONIO

EMPLOYEE ACKNOWLEDGMENT FORM
FOR

ADMINISTRATIVE DIRECTIVE 7.5
Acceptable Use of Information Technology

Employee:

I acknowledge that on _____, 20____, I received a copy of Administrative Directive 7.5 Acceptable Use of Information Technology. I understand if I should have any questions I should contact my Human Resources Generalist.

_____	_____
Employee Name (Print)	Department
_____	_____
Employee Signature	SAP ID #