Computer & Network Acceptable Use Policy

Policy:

The Information Technology Department is committed to protecting the City of Irving's computing and networking infrastructure from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing e-mail, web browsing, are the property of City of Irving. These systems are to be used for business purposes in serving the interests of the City, and of our employees and citizens in the course of normal operations.

Effective security is a team effort involving the participation and support of every City of Irving employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose:

The purpose of the Computer and Network Acceptable Use policy is to:

1. Make certain that all City of Irving computer and network resources are used for purposes appropriate to City of Irving business;

2. Inform all employees, consultants, contractors, vendors, interns, volunteers and any other authorized user of City of Irving about the applicability of laws and policies to computer and network usage;

3. Establish policies on privacy, confidentiality, and security in electronic communications; and

4. Provide guidance concerning rights and responsibilities with respect to the proper use of City of Irving computer and network resources.

Scope:

The Computer and Network Acceptable Use Policy applies to:

1. All authorized users of City of Irving include but not limited to all employees, consultants, contractors, vendors, interns, volunteers and other workers at City of Irving from third party entities;

2. All computer and network resources leased, owned, or managed by City of Irving and its contractors and consultants.; and

3. All electronic communications records in the possession of City of Irving authorized users.

Roles And Responsibilities:

City of Irving Responsibility: The City of Irving retains the power and authority to specify who uses its equipment and the information contained therein, under what circumstances, and to what purpose. Equipment and software purchased by the City belongs to the City, and City employees have no ownership rights to any equipment or software issued or loaned to them by the City. The City of Irving retains the power and authority to move or reassign equipment as needed.

Department Director Responsibility: Department directors shall ensure that authorized users, which include each employee, consultant, contractor, vendor, intern, volunteer and any other authorized user in their department, receive a copy of the current policy and procedures for regulating the use of computers and the network, and that each user completes and signs acknowledgment of receipt of the current policy. Directors shall have oversight and responsibility for third party users: consultants, contractors, vendors and non-employee users in their departments. Department directors shall ensure that all third party users sign the third party network connection agreement and non-disclosure agreement prior to allowing access to any network resources. Directors shall coordinate any non-employee use in advance with the Information Technology Department. The department director may request Internet or e-mail access for employees in their department based upon the business necessity of the department. The department director or designee will review and refer all requests for downloading of non-City software from the Internet to Information Technology. Department directors are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, authorized users should consult with their supervisor, manager, or department director. The department director should review departmental use of the Internet and e-mail. They may revoke an employee's access to such systems at any time for any misuse of the systems or violation of this policy.

Information Technology Director Responsibility: The Information Technology Director shall be responsible for recommending updates of this policy, as necessary.

Strategic Resources & Budget Director Responsibility: The Strategic Resources & Budget Director shall be responsible for reviewing, updating and distributing this policy.

Supervisor: Each supervisor should review employee use of the Internet and e-mail, and may recommend to the department director that an employee's access to the Internet and

e-mail be revoked. The supervisor is responsible for communicating this policy and ensuring their staff is in compliance.

Authorized Users: All users granted computer and network resources are responsible for adhering to the intent of this policy and following procedures stated herein. Authorized users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, authorized users should be guided by departmental policies on personal use, and if there is any uncertainty, authorized users should consult their supervisor, manager, or department contact. The use of city equipment or software for private or personal gain is strictly prohibited. Authorized users shall have the sole responsibility to safe guard portable computing devices assigned by the City of Irving. Care must be taken in reducing the possibility of loss of these devices both in the office and out. Your portable devices shall not be shared and must be kept in a safe and secure area where it may not be damaged. Any authorized user who becomes aware of misuse or abuse of computer or network systems must promptly contact his or her supervisor or department contact. If an authorized user mistakenly accesses restricted material he or she must immediately notify a supervisor, the helpdesk or the Network Security Specialist so that this material may be blocked from further access. Each authorized user is personally responsible for the content of his or her Internet and e-mail use. All authorized users are herby informed that use of the Internet and e-mail is not confidential and each authorized user's activities may be monitored at any time. Authorized users will use the Internet and e-mail system for work related matters; however, personal e-mail is permitted on a limited basis as long as such e-mail does not otherwise violate this or other applicable City or departmental policies. Authorized users are forewarned that all electronic documents are stored based on the City of Irving retention policy and subject to the Texas Open Records Act. In addition, personal emails of City of Irving authorized users may be subject to Texas Open Records Act if used for business purposes.

Third Parties: All consultants, temporary employees, contractors, vendors, interns, and volunteers, referred to as third party users, are responsible for adhering to the intent of this policy and following the procedures stated herein. All third party users must additionally sign a third party network connection agreement before accessing any of the City of Irving's network systems.

Information Technology: The Information Technology Department is responsible for setting up employee accounts to use the Internet, e-mail, and other network resources. Information Technology must approve all downloading of non-City software from sources via the Internet. All violations uncovered through the auditing or investigations by Information Technology will be reported to the Strategic Resources & Budget Director for resolution.

Confidentiality and Security:

Confidential or sensitive data as defined by governing agencies of the City shall not be sent over the Internet or e-mail without the use of an encryption medium approved by the Information Technology Director. Texas law requires authorized users protect the integrity of the City's confidential information as well as the confidentiality of others. Each authorized user is required to understand and comply with the following provisions:

1. All materials sent or received over the Internet shall be considered property of the City. An authorized user does not have privacy rights in any matter created, received or sent. The City reserves the right to monitor access or disclose any message created, received or sent via the Internet or e-mail at anytime, without advanced notice.

2. Authorized users must comply with all other personnel policies and procedures of the City and all established departmental practices or directives. For employees, violations discovered by monitoring or auditing activities, may be grounds for disciplinary action, up to and including dismissal. Additionally, illegal activity discovered may be brought to the attention of the appropriate law enforcement agency.

3. Electronic messaging systems, as well as other computer systems, are subject to the right of discovery in legal actions brought against the City. Additionally, electronic messages may be subject to disclosure under the Texas Open Records Act.

4. Authorized users are responsible for their individual computer accounts and shall take all reasonable precautions to prevent others from using their accounts. All PCs, notebooks and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less. Authorized users without a password protected screensaver shall log off each time they leave the computer unattended. All authorized users will log off at the end of their work shift unless instructed otherwise. Account owners are ultimately responsible for all activity under their account..

5. Authorized users will immediately notify their supervisor, an Information Technology manager, the helpdesk or the Network Security Specialist if they become aware of any violation of this policy.

6. Authorized users will not connect, attempt to connect or disconnect any computer or peripheral to, from or within the City of Irving network without prior authorization from the Information Technology Director.

7. Removable or portable devices should not be connected to City of Irving computer and network resources unless the device is approved by Information Technology

Director. Approved devices should utilize an approved encryption mechanism with a public and private key and files password protected.

8. Authorized users will not use or attempt to use on the City of Irving network any of the following items: any computer operating system media; computer or network utilities; network monitors; unlocking utilities or any software used to repair, change or monitor computer operations, network activity or security.

9. No authorized user will use a City of Irving password to access any city accounts from outside or inside the City of Irving network unless either specifically authorized by his or her department director, or unless such account is available to the public.

10. It is recommended that authorized users incorporate confidentiality disclaimers in emails sent to third parties.

11. Authorized users shall not write down passwords to City of Irving resources in an insecure area.

12. Password policies for City of Irving computer and network resources will be further governed by the City of Irving Global Security Policy.

13. Confidential information should not be downloaded or stored on portable resources unless proper encryption and password protection mechanisms are in place.

Unacceptable Use:

The following activities are, in general, prohibited. Authorized users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an authorized user permitted to engage in any activity that is illegal under local, state, federal or international law while utilizing City of Irving-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

1. Violations of the rights of any person or company protected by 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 City of Irving.

2. Accessing or viewing sexually explicit or pornographic material.

3. Unauthorized copying of copyright material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which City of Irving or the authorized user does not have an active license is strictly prohibited.

4. Exporting software, technical information, public safety information, or encryption software, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) that may gain unauthorized access to any computer or computing system and cause intentional disruption.

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a City of Irving computing asset to actively engage in procuring or transmitting material that is in violation of discriminatory, sexual harassment or hostile workplace laws.

8. Making fraudulent offers of products, items or services originating from any City of Irving account.

9. Effecting security incidents or disruptions of network communication. Security incidents include, but are not limited to, accessing data of which the authorized user is not an intended recipient or logging into a server or account that the authorized user is not expressly permitted to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited.

11. Executing any form of network monitoring which will intercept data not intended for the authorized user’s host, unless this activity is part of the employee’s normal job/duty.

12. Circumventing user authentication of security of any host, network or account.

13. Interfering with or denying service to any user other than the authorized user's host (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Unless explicitly authorized by the Information Technology Director, providing information about, or lists of, City of Irving employees or its affiliates to parties outside City of Irving.

16. Authorized users shall not conduct personal business or practices of any type that are intended for personal gain or misuse the systems for recreational purposes.

17. Authorized users shall not incur personal charges through the use of these systems. In the event that an employee does incur personal charges, through the use of these systems, that employee will be responsible for reimbursing the City for all expenses incurred.

18. Security software (i.e. firewalls, anti-virus, anti-spyware, etc) shall not be removed or disabled by an authorized user for any reason.

E-mail Activities

1. Authorized users shall not access their personal e-mail accounts through the City's Internet system. Locally installed network devices used for personal Internet provider access is prohibited without the prior approval of the Information Technology Director.

2. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

3. Forging or masking the sender e-mail address to misrepresent the origin/sender.

4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters" or other "pyramid schemes" of any type.

6. Use of unsolicited e-mail originating from within City of Irving's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service

hosted by City of Irving or connected via City of Irving's network.

7. Posting the same or similar non-business-related messages to large numbers of Internet forums and web sites.

8. Authorized users shall not attempt to access or read e-mail received by another employee without prior authorization from the City Manager's Office or the Strategic Resources & Budget Director. Any such access will be coordinated through the Information Technology Director. The Information Technology Director may designate key personnel to monitor e-mail for abuse and troubleshooting purposes.

9. Sending and receiving encrypted messages must be approved and agreed upon by the Information Technology Director prior to sending or receiving such messages.

10. Authorized users receiving e-mail containing '.zip' or '.exe' files and other executable attachments are responsible for informing Information Technology before opening any such files.

11. It will be the responsibility of the email sender to retain emails for permanent record when sent to third parties.

12. Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user to otherwise deceive recipients as to the content of the originating sender's e-mail.

Instant Messaging (IM)

1. Authorized users are strictly prohibited from downloading/installing/using any Instant Messaging (IM) software without specific authorization in writing from their respective Department Director and the Information Technology Director. Authorized use of instant messaging are subject to review and approval on a case by case basis. Information Technology department is responsible for setting technology standards with respect to Instant Messaging software and protocols. Unauthorized use of instant messaging software by employees may be subject to disciplinary action, up to and including dismissal.

Blogging Activities

1. Blogging by authorized users, whether using City of Irving's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of City of Irving's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate City of Irving's policy, is not detrimental to City of Irving's best interests, and does not interfere with an employee's regular work

duties. Blogging from City of Irving's systems is also subject to monitoring.

2. Authorized users are prohibited from revealing any City of Irving confidential or proprietary information.

3. Authorized users shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of City of Irving and/or any of its employees. Authorized users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by City of Irving's Non-Discrimination and Anti-Harassment policy.

4. Employees may also not attribute personal statements, opinions or beliefs to City of Irving when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of City of Irving. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, City of Irving's trademarks, logos and any other City of Irving intellectual property may also not be used in connection with any blogging activity.

Respecting Resource Limits:

1. Authorized users will adhere to any instructions that are given to them by Information Technology personnel regarding network or computer use.

2. Music, image, or video files will only be stored and/or accessed for a business purpose and with the authorization of the authorized user's department director. Examples include, but are not limited to, transmission of MP3 files or data transmission of video files. Authorized users will not store music, image, or video files after the files are no longer needed for business purposes.

Disciplinary Action:

An employee or third party user found to be in violation of this policy, or applicable state or federal laws, is subject to the loss of computer and network privileges and/or additional disciplinary actions, up to and including dismissal.

Definitions:

Attachment: An attachment includes any file that is included with or attached to an electronic communication between an originator and a receiver.

Authorized User: Any person who uses the City of Irving computing resources with proper authorization from City of Irving Information Technology. This includes all employees, consultants, contractors, vendors, interns, volunteers, and other personnel from third party entities.

Blogging: The practice of posting entries in your weblog. A weblog (usually shortened to blog, but occasionally spelled web log) is a web-based publication consisting primarily of periodic articles (normally in reverse chronological order).

Chain E-mail: A message sent to one or more recipients requesting each to write or forward similar letters to a specified number of other recipients and often employed as a moneymaking scheme.

City of Irving network: A network which is compromised of the City's computing and network infrastructure. This term includes each personal computer owned by or leased to the City of Irving, regardless of whether it is connected to any network system, as well as each peripheral apparatus, such as, but not limited to printers, routers drives, wiring and cabling. The City of Irving network may also provide access to other public networks and the Internet.

Denial of Service (DOS) Attack: A method of attacking a server by sending an abnormally high volume of requests over a network, which essentially slows down the performance of a server, such that the server is unavailable for Authorized Users.

Email Bomb: An email bomb is characterized by abusers repeatedly sending an email message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact.

Email Spoofing: Spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

Extranet: A secure extension of an organization's network, typically over a virtual private network (VPN) tunneling through the public Internet, to share designated information or operations with users outside the organization; for example, suppliers, vendors, consultants, and contractors might make use of an extranet.

Forged Routing Information: Routing information which is misleading or incorrect or which would tend to disguise the origin of the routed material. Usually refers to information that is not generated by any routing device (such as a mail server), but is inserted by a party using software which is designed to produce false routing information (headers in the case of E-mail).

Instant Messaging (IM): is a tool like email that allows a form of text based communication from one person or persons to another.

Internet: The Internet is a worldwide system of computer networks that allows users to send and receive information from other computers.

Intranet: A computer network, based on Internet technology that is designed to meet the internal needs for sharing information within a single organization.

Malicious Programs: Viruses, worms, Torjan horses, and spyware are different types of malicious programs. It can be transmitted in attachments to an email, by downloading infected programming from other sites, and can be present on a removable device.

Packet Sniffing: Within a given network, a network device can be used to capture and analyze network traffic. Within a network, username and password information is generally transmitted in clear text or unencrypted format. Information can easily be captured using a sniffer by a malicious intruder.

Packet Spoofing: Emitting a network packet with a source address you do not have permission from the owner to use.

Phishing: A phish is an email message that is designed to appear as though it came from a financial institution, government agency or commercial site and is intended to deceive the user to revealing sensitive information like social security number and passwords.

Ping Flood: A ping flood is a simple Denial of service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets. It only succeeds if the attacker has more bandwidth than the victim (for instance an attacker with a DSL line and the victim on a dial-up modem). The attacker hopes that the victim will respond with ICMP Echo Reply packets, thus consuming outgoing bandwidth as well as incoming server bandwidth.

Pyramid Scheme: A fraudulent scheme in which people are recruited to make payments to the person who recruited them while expecting to receive payments from the persons they recruit; when the number of new recruits fails to sustain the hierarchical payment structure the scheme collapses with most of the participants losing the money they put in.

Spamming: Using a computer or other electronic device to send an unsolicited advertisement to an electronic mail address.

Acknowledgement:

If you have questions about the above policies and procedures, address them to Strategic Resources & Budget or Information Technology before signing the following agreement.

I have read the City of Irving's Computer and Network Acceptable Use Policy and agree to abide by it. I understand that a violation of any of the above policies or procedures may result in disciplinary action and/or loss of computer and network privileges. Additionally, City of Irving shall not be responsible for any damages that the authorized user may suffer arising from or related to the use of City of Irving computing resources.

_____
Name

_____
Signature

_____
Date

Note: All third party users must additionally sign a third party network connection agreement before accessing any of the City of Irving's network systems.

File Name:

W:\IT Policy\Draft\Security\Computer and Network Acceptable Use Policy.doc

Revision History

Date	Revision	Description
28/03/2008	1.3	Approved by IT Management
11/15/2007	1.2	Further revisions following IT review
11/05/2007	1.1	Revisions following IT review
10/18/2004	1.0	Initial creation