CITY of AUSTIN Administrative Bulletin

Title: **Acceptable Internet Use**

Administrative Bulletin Number	**98-06**
Effective Date	
Revised	___ Annually **x** As Needed
Prepared by	Communications and Technology Management
Original Date	November 18, 2006
Revised	November 27, 2007
Manager's Approval	Toby Hammett Futrell

PURPOSE

The purpose of this policy is to establish guidelines and minimum requirements governing the acceptable use of City-provided Internet, electronic mail (e-mail) and computer use.

Internet and e-mail resources are provided to support:

- Internal communication between employees
- External communication between employees and people with whom they need to interact to perform their jobs
- Collaborative work among working groups
- Information about the activities and services of the City of Austin
- Delivery of City of Austin services in electronic form
- Research and education

This policy applies to any person(s) and/or contractor(s) (hereinafter referred to as "users") whose access to or use of Internet, electronic mail and/or computer use is funded by the City or is available through equipment owned or leased by the City.

POLICY

The use of City-provided Internet, e-mail and/or computer use must be related to, and for the benefit of, City government.

All on-line communications, such as electronic mail messages (and attachments) and postings to various kinds of discussion groups, are subject to the same laws, regulations, policies, and other requirements as information communicated in other written forms and formats. This includes proper business correspondence practices and proper use of City of Austin equipment and resources.

Use network resources responsibly to avoid having a negative impact on others who need to share those resources (see the resource considerations section below).

For examples of acceptable and unacceptable use, see the acceptable use and unacceptable use sections below.

DEFINITIONS

Definitions for this Administrative Bulletin and all other computer related security bulletins and policies can be found at:

http://cityweb.ci.austin.tx.us/ctm/security/terms_contacts.cfm.

ROLES AND RESPONSIBILITIES

Department:

All City departments are responsible for the Internet and electronic mail activities of their users. City departments have the responsibility to ensure that usage of City-provided Internet and e-mail services serves legitimate government functions and purposes. Managerial authority over use of these services should be defined within each department. User information that addresses Internet and electronic mail usage and policies should be disseminated.

Departments may provide additional restrictions and guidelines regarding the use of the Internet and electronic mail within their local environments. In considering the need for additional restrictions and guidelines, each department may take into account its particular needs, mission, available technology, level of staff training, size, geographic diversity, and organizational culture.

Users: Each user has the following responsibilities:

- Comply with this "Acceptable Use Policy." By participating in the use of networks and systems provided by the City, users agree to comply with City and department policies governing their usage.
- Do not download and/or install non-authorized software on your PC.
- Take all reasonable precautions to prevent the use of their electronic mail account and their workstation by unauthorized individuals. Lock or use a screen saver password whenever you leave your PC to protect your account from unauthorized access.
- Users are responsible for activity from their login account, email account and/or their workstation.
- Comply with other City and department policies, procedures, and standards.
- Be courteous and follow accepted standards of etiquette and "netiquette".
- Use information technology resources efficiently and productively.
- Communicate data security needs of information under your purview to your LAN administrator or ctm.security@ci.austin.tx.us.
- All desktops must have up to date virus protection installed and active.
- All servers should have up to date virus protection. If you feel like you have a server that does not require it, please email ctm.security@ci.austin.tx.us for authorization.
- Save all business data to authorized drives that ensure backups are done appropriately.

CORRESPONDING PROCEDURES AND POLICIES

City of Austin Acceptable Use Policy - CTM Website

http://cityweb.ci.austin.tx.us/ctm/security/user/acceptable_use.cfm.

City of Austin Information Security Policies – CTM Website

http://cityweb.ci.austin.tx.us/ctm/security/index.cfm.

PROCEDURE

Implementation:

Security:

- Transmission of electronic mail to locations outside of the City's internal mail system may require the use of the Internet for transport. Since the Internet and its tools adhere to open and documented standards and specifications, it is inherently an unsecured network that has no built-in security controls.
- Although confidential and sensitive information should not be included in electronic mail and on-line communications unless proper, formalized security precautions have been established (e.g. encryption), certain electronic mail communications may be privileged or confidential. It is the responsibility of each City department to protect confidential and sensitive information where intentional, inappropriate, or accidental disclosure of the information might expose the City or an individual to loss or harm. Please contact CTM's Security Engineering for assistance.

- Do not share passwords. Do not give your password to anyone. Authorized users will be able to get your password through legitimate means. (For example: If your IT person needs to access your account, they have the rights to change your password.) You are responsible for your login account and password. Here are hints at picking good passwords:
    - **Use a good password.** Most users choose their password. Keep these guidelines in mind when you choose a password.
    - It is recommended that you use an 8 character password. Adding a character dramatically increases the strength of your password.
    - Use UpPeR and LoWeR case letters. Use special characters like !@#%^&&**_"><__ (Think of when cartoons are cussing - these are special characters.) Use letters and numbers.

        - Examples of Good Passwords: Luv4U1sOK (love for you is OK), Ok4j@mm! (ok for jamming), b0BS@v31T (bob save it) ...etc.
        - Examples of Bad Passwords: bob061169, Austin12, football, fluffy, 123456, cheryl31, futrellt, ...etc.
        - Tip: try using phrases, it makes cracking them hard and they are fairly easy to remember.

- Here is where poor spelling is your friend! Don't use a dictionary word or a personal name - no matter what language. Hackers have databases of dictionary words, and personal names in all languages to test against your account.
- Don't stick your password under your keyboard, mouse pad or on your monitor.

- Telnet use is not recommended because the password goes over the Internet in clear text so that anyone can read it. SSH is encrypted Telnet and is recommended. If Telnet is your only option, do not use the same password on these accounts as you do on your City accounts.
- Internal instant messaging is allowed but external instant messaging will be blocked.
- Access restricted through the use of security levels as defined in CTM Physical Security Levels Policy The CIO will define security levels that will be used to partition security environments, both physical and logical, throughout the City.

Privacy:

Neither Internet usage nor electronic mail messages are personal or private.

All computer files are the property of the City of Austin, regardless of their physical location or the form in which they are maintained. The City of Austin reserves the right to access and disclose all messages and other electronic data, sent over its electronic mail system or stored in its files, for legal and audit purposes. Under the Texas Open Records Act, any electronic mail can be a public record. Employees should be aware that electronic records are subject to the mandatory public disclosure requirements of the Texas Open Records Act, subject to the exceptions under the Act.

E-Mail is backed up daily on a permanent basis allowing the City of Austin to restore current electronic mail in the event of system failure. Employees should assume that copies (back-up copies or otherwise) of electronic mail messages and other electronic correspondence may exist on other systems even though the sender and recipient have discarded their copies of the document.

Information Systems Department monitors every connection to the Internet (all email, web sites, instant messages ...etc.)

Acceptable Use:

Acceptable uses of computer resources are those that conform to the purpose, goals, and mission of the department and to each user's job duties and responsibilities. The following list, although not all-inclusive, provides some examples of acceptable uses:

- Communications and information exchanges directly relating to the mission, charter, and work tasks of the department including electronic mail in direct support of work-related functions or collaborative projects.
- Communications with vendors of products used or being considered for use by the City, either to investigate use of their product or to receive help in using their product.
- Communications, including information exchange, for professional development or to maintain job knowledge or skills.
- Announcements of City laws, procedures, hearings, policies, services, or activities.
- Use involving research and information gathering in support of the City's governmental duties.

Unacceptable Use:

Unacceptable use can be defined generally as activities that do not conform to the purpose, goals, and mission of the department and to each user's job duties and responsibilities. Any computer usage in which acceptable use is questionable should be avoided. When in doubt, seek policy clarification prior to pursuing the activity.

The City of Austin computer use, e-mail and/or Internet access may not be used to:

- Listen to, view, or download audio or video files for entertainment or leisure activities. These activities are bandwidth intensive and take resources away from our customers.
- Seek or gain unauthorized access to City of Austin network resources or to Internet resources.
- Destroy the integrity of computer based information.
- Compromise the privacy and/or security of users.
- Disrupt the functions of City of Austin networks or other computer resources, including, but not limited to, propagation of worms or viruses or other debilitating programs.
- Conduct or participate in illegal actions.
- Violate City of Austin or department policies.
- Circumvent legal protection provided by copyright and license to programs and data.
- Conduct or promote commercial or private/personal business enterprises or products.
- Engage in political lobbying.
- Support or solicit on behalf of groups, organizations, etc. that are not related to City of Austin.
- Transmit unsolicited commercial information (i.e. junk mail, advertising, etc.)
- Transmit material that may be deemed offensive to its recipient.
- View, transmit, or receive sexually explicit material.
- Advocate racial, ethnic, religious, or gender-based slurs.
- Threaten or harass others.
- Harm to minors.
- Threats.
- Harassment.
- Fraudulent activity.
- Forgery or impersonation.
- Unsolicited email or bulk email.
- Unauthorized access.
- Copyright or trademark infringement.

The City of Austin realizes that we have little control over communications received, especially those received from unsolicited sources. Any unsolicited electronic correspondence (Spam) received should be disposed of accordingly. Click here to find out more about Spam.

Capability Specific Policies:

The following policies relate to specific types of interaction.

E-Mail (Electronic Mail)

- Theft and forgery (or attempted forgery) of E-mail messages is prohibited.
- Sending chain letters is prohibited.

- City of Austin employees who have been provided E-mail capability have an obligation to read incoming messages in a timely manner and respond accordingly.

Listservs, Mailing Lists, and Discussion Groups

- Unsubscribe to all mailing lists upon a change in your e-mail address or when you leave City of Austin employment

Downloading files using FTP (File Transfer Protocol)

- Check for copyright or licensing agreements when downloading files.
- DO NOT type in your network or Internet password when utilizing "Anonymous FTP". Instead, type in your E-mail address when the FTP site requests a "Password".

World Wide Web (WWW)

- Employee (non business related) Web pages and Web sites are not permitted on the City of Austin system.
- Development and management of City department Web pages must be coordinated through the Austin City Connection Group.

Remote Access, Telework, dial-up, VPN, RAS

- Remote access is a privilege not a right. Any violation in its use will result in access being terminated.
- Do not share connection information with anyone. This includes passwords, shared secrets, phone numbers, encryption keys or software.
- Do not create connections to non-COA networks without permission from the COA Security Supervisor.

Wireless Network/Access

- Wireless connections to the City of Austin network must be approved by Security before deployment. For approval, make an CTM Help Desk request (512-974-HELP or helpdesk@ci.austin.tx.us). It is advisable to consult Security BEFORE purchase to make sure the wireless application meets security thresholds.
- Wireless home networks are not allowed to be connected to the city's network while teleworking.

Resource Considerations:

The following policies relate to activities that may negatively affect network performance and resources.

- Do not broadcast messages to all City employees at once.
- Delete unnecessary e-mail communications, but do not violate City record retention requirements. Each user account has a set limit (50MB for CTM supported units) which users will not be able to accumulate more than that amount. Call your help desk for your specific limits and your help desk can also advise you on how to store email in other locations if you need it.
- Whenever possible, avoid sending e-mails with large attachments. For internal correspondence, it is preferable to place the document in a shared location and reference

it in the e-mail. When sending or receiving a large file via the Internet, use FTP instead of using attachments to email. (File-transfer protocol is the program that is used to transfer large files over the Internet.)

- Limit downloads, especially large files, to a time after normal business hours (consider both local time and the time at the remote site), except in an emergency. Users must be knowledgeable about the resource requirements for the file transfer both in terms of the network and of the desktop's capacity.
- Don't subscribe to very active mailing lists, discussion groups or news groups unless absolutely necessary. They can flood your mailbox with several hundred messages a day, impacting both your time and the network's resources. Out of Office notifications can cause looping where mailing lists constantly email you and you constantly email them until it is turned off.
- Avoid web sites with very large graphics as they can be very high bandwidth consumers.
- Avoid viewing (or listening to) large multimedia (sound, picture, and video) files.
- Streaming video and audio can saturate a network so that no one can do work. You will not be allowed to use streaming video or audio for leisure activities.
- On-line communications, depending on the method employed, may utilize enormous amounts of bandwidth, and therefore, care should be taken when accessing these resources.
- Do not download music for entertainment purposes. These peer to peer music swapping programs have virus, copyright and bandwidth issues. We need to preserve our Internet bandwidth for servicing our customers.

Sanctions:

Workforce members who violate the information security policies of the City will be subject to loss of City resources and/or disciplined in accordance with the severity of the infraction and pursuant to the City's personnel policies.

The penalty for violation of this Administrative Bulletin is outlined in the Information Security Sanctions Policy at: http://cityweb.ci.austin.tx.us/ctm/security/user/sanctions.cfm.

FORMS

Security Related Forms

- Third Party Connection Request Form
- Third Party Connection Migration Checklist
- CTM Non Disclosure Form