

Memorandum

Date: May 13, 2008
RE: Proposed Alterations of Email Policies

The following document outlines an extensive and fair email policy that outlines clear guidelines for city employees and its contractors. The Mayor's Office of Technology strongly recommends these policies be adopted in order to save the city money in data storage space and in order to protect the city's interest in providing a secure work environment.

According to the Florida League of Cities, "in a survey of over 800 workers, 31 percent of those surveyed admitted to sending out confidential information via e-mail; 55 percent admitted to exchanging racist or sexist e-mails; and 60 percent admitted to having sent or received adult-oriented material." These types of emails increase potential liability for the city and go against city harassment policies.

More and more lawsuit involving e-mails and cases show that not having proper procedures in practice have deep legal ramifications. Employers are almost always held responsible for email transmissions.

Further, strong policies prevent confidentiality breaches, damage to reputation (i.e. someone uses a city account to email offensive statements or offensive posts to blogs), and loss of productivity.

As employees download more and more videos and photos from the web, the needed space to store vital data is threatened. Moreover, as the city prepares to pay for housing backups of data outside the city, the city risks paying for its employees personal downloads to be stored as well.

As with all policies and procedures, the e-mail policy should be made easily accessible to all city employees. We strongly encourage the adoption of the following policies and the distribution to all employees and contractors working in city government.

**Email Guidelines and Policies for
The City of New Orleans**

TABLE OF CONTENTS

A. Overview.....	4
B. City Of New Orleans Acceptable Use Policy	4
1.0 Overview	4
2.0 Purpose	4
3.0 Scope.....	4
4.0 Policy	4
5.0 Enforcement	8
6.0 Definitions.....	8
C. Automatically Forwarded Email Policy	8
1.0 Purpose	8
2.0 Scope.....	8
3.0 Policy	8
4.0 Enforcement	8
5.0 Definitions.....	8
D. Email Retention Policy.....	9
1.0 Purpose	9
2.0 Scope.....	9
3.0 Policy	9
4.0 Enforcement	10
5.0 Definitions.....	10

City of New Orleans' Email Policies

A. Overview

The following sections state the City of New Orleans' Email Policies for Acceptable Use, Forwarded Email, and Email Retention. These policies apply to employees, consultants, temporaries, and other workers at the City of New Orleans.

B. City Of New Orleans Acceptable Use Policy

1.0 Overview

Our intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to City of New Orleans established culture of openness, trust and integrity. The City of New Orleans commits to protecting its employees and partners 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 electronic mail, WWW browsing, and FTP, are the property of City of New Orleans. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every City of New Orleans' 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.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at City of New Orleans. These rules are in place to protect the employee and City of New Orleans. Inappropriate use exposes City of New Orleans to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at City of New Orleans, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by City of New Orleans.

4.0 Policy

4.1 General Use and Ownership

1. While City of New Orleans's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of City of New Orleans. Because of the need to protect City of New Orleans's network, management cannot guarantee the confidentiality of information stored on any network device belonging to City of New Orleans.
2. Employees 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.

3. The City of New Orleans recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within City of New Orleans may monitor equipment, systems, and network traffic at any time.
5. City of New Orleans reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts.
 - a. Authorized users are responsible for the security of their passwords and accounts.
 - b. System level passwords should be changed quarterly.
 - c. User level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Employees are prohibited from posting from a City of New Orleans' email address to newsgroups, unless posting is in the course of business duties.

4.2.1 Virus and SPAM Control

All hosts used by the employee that are connected to the City of New Orleans Internet/Intranet/Extranet, whether owned by the employee or City of New Orleans, shall be continually executing approved virus-scanning software with a current virus database.

4.2.2 Attachment Filters

The Internet Mail Gateway is currently configured to block incoming attachments with the following file extensions:

.ade	.com	.inf	.mst	.vb
.adp	.cpl	.ins	.nsw	.vbe
.asp	.crt	.isp	.pcd	.vbs
.asx	.dll	.js	.pif	.wav
.bat	.eml	.jse	.rar	.wsc
.bin	.exe	.mp3	.reg	.wsf
.chm	.hlp	.msi	.scr	.wsh
.cmd	.hta	.msp	.shs	

The City of New Orleans reserves the right to apply filters on certain types of files if the file type in question poses a risk to resources on the network.

4.2.3 Quarantine

These incoming files will be quarantined for 7 days. .vsd .zip. Customers will be notified that an attachment was quarantined and may request that attachments be forwarded to their inbox. This will allow customers to receive work related attachments while protecting them from potentially malicious attacks.

4.2.4 3rd Party Messaging Applications

Email applications such as AOL Instant Messenger, Microsoft HotMail and any other free web-based/instant messaging email products are a security risk to an agency's network and to the citywide messaging network. Much time and expense has been invested in ensuring that messages are free from virus attacks. Messages from products such as Instant Messenger and Hotmail are not scanned for viruses or malicious program; therefore these programs provide a backdoor for intrusions and infections. As such, these products put the entire citywide messaging system at risk by exposing the network to potential

malicious code. In addition to these risks, the installation of these applications often causes other desktop applications to malfunction. For these reasons, 3rd party messaging applications are prohibited unless approved by the Mayor's Office of Technology.

4.2.5 Maintenance

Scheduled Maintenance

Scheduled maintenance shall mean any maintenance on the messaging network to which User's network is connected 1) of which User is notified, or 2) that is performed during a standard maintenance window on Sundays from 6 PM to 12 AM. Notice of Scheduled Maintenance will be provided to Customers by email message.

Backups

A full backup is run every night on the messaging server database. Tapes are stored offsite for 30 days. Backups are not intended to be used to restore messages that were accidentally deleted. These backups are used to restore corrupted databases, recreate the email environment in the case of a disaster, and retain an archived (30 days) copy in the event proper authorities request information.

Restores will require 1) a written request by agency upper management, and 2) approval by the Mayor's Office of Technology. Special charges will apply for user-requested restores. Only files stored on the citywide messaging server will be backed up. Personal (.PST) and offline (.OST) folders on the departmental computers will not be backed up.

4.3 Storage and Transaction Limitations

Amount of storage on the mail server by default is set to 50 MB per user. Remember, storage includes Inbox, Sent Items, Deleted Items, Calendar, Tasks and Contacts. Larger storage limits can be configured, but will require approval by agency appointed authority since additional storage may increase agency costs.

1. Warning notifications are sent when you are within 5 MB of your limit.
2. Sending email is prohibited when a mailbox exceeds the storage limit.
3. Maximum send size is 15 MB per message.
4. Maximum receive size is 15 MB per message.
5. Exceptions to these limits will be considered on a business case basis.

4.4 Age Limits

The following age limits are set on messages stored on the email system:

1. Inbox - No age limit. Removed only by mailbox owner.
2. Sent Items - No age limit. Removed only by mailbox owner.
3. Deleted Items - 7 Days
4. Deleted item retention is 7 days. (Mail deleted from Deleted Folder is held for 7 days.)

4.5 Authentication

To eliminate dual logons, a domain trust relationship can be configured and maintained. The trust will also allow customers to enforce their own password policies and administration. Agencies that choose the no trust option are subject to the City Email password policy, as follows:

1. Maximum age: 30 days
2. History: 5
3. Complexity: 3 out of 4 of the following characters: Uppercase, lowercase, numbers or symbols

4.6 Account Creation Standards

1. Names in the Address List will be displayed as "Firstname Lastname". Duplicate names will be distinguished by the use of an agency identifier. (Example: "Firstname Lastname -DPS")
2. The Company field is used for City agency name and must be completed for each user profile.
3. The Department field is optional if an agency wants to distinguish different sections for billing purposes.
4. 10 digits must be used in the phone number. (Example: 225-555-5555)

4.7 Unacceptable Use

The following activities are, in general, prohibited. Employees 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 employee of City of New Orleans authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City of New Orleans-owned resources.

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

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

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 New Orleans.
2. Unauthorized copying of copyrighted 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 New Orleans or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, 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.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. 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.
6. Using a City of New Orleans computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any City of New Orleans account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized 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 unless prior notification to the City is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee'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. Providing information about, or lists of, City of New Orleans employees to parties outside City of New Orleans.
16. Using any messenger programs (i.e. AIM, Microsoft Messenger, Trillion etc ...) or personal profile spaces to include (MYSPACE, FACEBOOK, HOTMAIL, MATCH, ETC ...).
17. Employees may view video from You Tube or other similar programs only if they pertain to the City of New Orleans' business. These videos should not be saved without approval from the Mayor's Office of Technology.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within City of New Orleans's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by City of New Orleans or connected via City of New Orleans's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated the above policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

<u>Term</u>	<u>Definition</u>
<i>Spam</i>	Unauthorized and/or unsolicited electronic mass mailings.

C. Automatically Forwarded Email Policy

1.0 Purpose

To prevent the unauthorized or inadvertent disclosure of sensitive company information.

2.0 Scope

This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of City of New Orleans.

3.0 Policy

Employees must exercise utmost caution when sending any email from inside City of New Orleans to an outside network. Unless approved by an employee's manager, City of New Orleans email will not be automatically forwarded to an external destination. Sensitive information will not be forwarded via any means, unless that email is critical to business and is encrypted.

4.0 Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

<u>Terms</u>	<u>Definitions</u>
--------------	--------------------

Email	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora and Microsoft Outlook use SMTP.
Forwarded email	Email resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to City of New Orleans or its customers' dollar value, reputation, or market standing.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

D. Email Retention Policy

1.0 Purpose

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to the Mayor's Office of Technology.

2.0 Scope

This email retention policy is secondary to City of New Orleans policy on Freedom of Information and Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All City of New Orleans email information is categorized into four main classifications with retention guidelines:

- Administrative Correspondence (4 years)
- Fiscal Correspondence (4 years)
- General Correspondence (1 year)
- Ephemeral Correspondence (Retain until read, destroy)

3.0 Policy

3.1 Administrative Correspondence

City of New Orleans Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox info@City of New Orleans has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

3.2 Fiscal Correspondence

City of New Orleans Fiscal Correspondence is all information related to revenue and expense for the company. To ensure Fiscal Correspondence is retained, a mailbox fiscal@City of New Orleans has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

3.3 General Correspondence

City of New Orleans General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

3.4 Ephemeral Correspondence

City of New Orleans Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

3.5 Encrypted Communications

City of New Orleans encrypted communications should be stored in a manner consistent with City of New Orleans Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

3.6 Recovering Deleted Email via Backup Media or re-managing for data recovery or Forensic reasons.

City of New Orleans maintains backup tapes from the email server and once a quarter a set of tapes is taken out of the rotation and they are moved offsite. No effort will be made to remove email from the offsite backup tapes. If data is needed for business continuity or Forensics the City State or Local government must designate a representative to re-manage the suspect account maintaining a strict chain-of-custody on said documents until the needs of the city our met.

4.0 Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms

Definitions

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here...]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within City of New Orleans is done via a license. Please contact the appropriate support organization if you require a license.

Approved Instant Messenger

The Jabber Secure IM Client is the only IM that is approved for use on City of New Orleans computers.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this

is accomplished by careful use of the `chmod` command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of City of New Orleans.

Encryption

Secure City of New Orleans Sensitive information. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your Page 11 of 11 manager and/or corporate legal services for further guidance.