Policy Statement

SUBJECT: City of Detroit Email Usage Policy

Contents

I. Overview

A. Purpose:

City of Detroit ("City") is committed to protecting the integrity, confidentiality and availability of its data and information assets. This policy:

- Describes email users' responsibilities for the proper use of City email service and potential consequences for failing to abide by these rules; Ensures users are aware of what the City deems to be acceptable and unacceptable use of email;
- Informs users that by using the City of Detroit email service the user agrees to comply with this policy and waives any right of privacy in any email they create, send, or receive using the City of Detroit email, or store in the City of Detroit email system; and
- Places users on notice that the City of Detroit can and may monitor use of email without prior notification, and that the City of Detroit reserves the right to take disciplinary action, including termination or legal action for failing to adhere to this policy

B. Audience/Scope:

This policy applies to any email message that is created or received by users of the City of Detroit electronic mail (email) service. Users of the City of Detroit email are employees or business partners (i.e. contractors or vendors) who have been issued a City of Detroit email address.

II. Detailed Email Usage Policy Provisions

A. General

1. The following activities are prohibited by policy:

    - Sending email that is intimidating or harassing.
    - Using email for conducting personal business
    - Using email for purposes of political lobbying or campaigning
    - Violating copyright laws by inappropriately distributing protected works
    - Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role
    - The use of unauthorized e-mail software

2. The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:

    - Sending or forwarding chain letters
    - Sending unsolicited messages to large groups except as required to conduct agency business
    - Sending excessively large messages (messages that would be longer than one page in a word document)

3. All sensitive City of Detroit material transmitted over external network must be encrypted.

    - Various encryption processes are available with ITS Guidance. Additionally ITS will assist in identification of information that may be considered, sensitive, confidential or Personally Identifiable.

4. All user activity such as websites visited, type of information accessed, code changes made on City of Detroit Information Technology System assets is subject to logging and review.

5. When using City of Detroit email all employees, who act in the scope of their employment are agents of the City

6. Individuals must not send, forward or receive confidential or sensitive City of Detroit data and information through non-City of Detroit email accounts. Examples of non-City of Detroit email accounts include, but are not limited to, Hotmail, Comcast, Yahoo mail, Gmail, AOL mail, and email provided by other Internet Service Providers (ISP).

7. Use of Mobile Device - If it is necessary for employees to send, forward, receive or store confidential or sensitive City of Detroit information and data employees must refer to the Mobile Device Policy. Examples of mobile devices include, but are not limited to, Personal Data Assistants, two-way pagers and cellular telephones.

8. Email storage size shall not exceed 2 gigabytes of data. When such limit is reached individual users are informed of it **3** number of times and asked to archive the emails and make room. If archival is not done after three warnings user's email traffic is blocked and will be forced to archive the emails and make room.

9. Encryption- City of Detroit reserves the right to use an encryption tool for all external email transmission

10. City of Detroit reserves right to monitor and report all the email activity of all employees

B. Prohibited

1. Any purpose that violates a federal or City government law, code or policy, standard or procedure

2. The advertising or other promotion of any private business enterprise or activity

3. Transmission or solicitation of information or statements that contain profane language, pander to bigotry, sexism, or other forms of prohibited discrimination, or can in any way be construed as intending to harass or threaten another individual, sexually or otherwise

4. Any activity with religious or political purposes outside the scope of the user's assigned and authorized governmental duties

5. Any unauthorized purchase

6. Sending email under names or addresses other than the employee's own officially designated City government email address

7. Adding, removing, or modifying identifying network header information ("spoofing") in an effort to deceive or mislead recipients

8. Employees are to not open any "executable" email attachments (e.g., .exe, .bat, .scr, .vbs) from any source

9. Sending or forwarding "chain" letters, i.e., those that ask the receiver to forward the message to multiple recipients

10. Sending any attachment files larger than 10 megabytes (MB). Exceptions to this rules must be approved by ITS

11. Sharing organized City email lists with any person outside the City, except as required by the Freedom of Information Act, subpoena, or other compulsory process

12. Setting email correspondence to forward automatically to an outside (non-City) address

13. Disruption, obstruction, or burden of network resources

14. The intentional or negligent introduction of computer viruses (or other malicious code) into any City of Detroit systems

15. Federal Tax Information is not to be emailed external to the City of Detroit email system

16. Transmission of sensitive (e.g., confidential) data and information unless protected by an approved encryption mode. This type of information includes:

    - PII - Personally Identifiable Information
    - PHI – Protected Health Information
    - FTI – Federal Tax Information

C. Instant Messaging

1. Employees, vendors or business partners are prohibited from downloading and using personal, consumer-grade IM (Instant Messaging) software (e.g., AOL Instant Messenger, Yahoo!, or MSN) to transmit messages via the public Internet

2. All IM communications, data and information transmitted, received, or archived in the city's IM system are assets to the City of Detroit

3. Employees have no reasonable expectation of privacy when using the city's IM system. The city reserves the right to monitor, access, and disclose all employee IM communications

4. The IM system is intended for business use only. Employees, vendors or business partners are prohibited from wasting computer resources, colleagues time, or their own time sending personal instant messages or engaging in unnecessary chat related to business

5. Treat IM messages as business records that may be retained and used as evidence in litigation, audits, and investigations

6. Always use professional and appropriate language in all instant messages. Employees are prohibited from sending abusive, harassing, threatening, menacing, discriminatory, pornographic, disrespectful, or otherwise offensive instant messages

7. Employees are prohibited from sending jokes, rumors, gossip, or unsubstantiated opinions via IM. These communications, which often contain objectionable material, are easily misconstrued when communicated electronically

8. Employees may not use IM to transmit confidential, proprietary, personal, or potentially embarrassing data and information about the company, employees, clients, business associates, or other third parties

9. Employees may not share confidential, proprietary, or potentially embarrassing business-related or personal IM with the media, prospective employers, or other third parties.

D. Malicious Code Support

Attachments to e-mails are a common method of distribution of malicious code. E-mail is inherently insecure due to its use of SMTP, a plain text-forwarding protocol, and its lack of strong authentication of message senders. The source of an e-mail address can be easily spoofed or falsified as someone that you trust. Often, this alone is enough to trick a recipient into opening an attachment

If you receive an attachment and need to determine if it is legitimate, you still need to verify it before opening it. Here are steps you can use to help you decide what to do with every email message with an attachment that you receive. You should only read a message that passes all of these tests.

The **Know** test: Is the email from someone that you know?

The **Received** test: Have you received email from this sender before?

The **Expect** test: Were you expecting email with an attachment from this sender?

The **Sense** test: Does email from the sender with the contents as described in the Subject line and the name of the attachment(s) make sense?

The **Virus** test: Does this email contain a virus? To determine this, you need to install and use an anti-virus program.

You should apply these five tests – **KRESV** – to every piece of email with an attachment that you receive. If any test fails, toss that email. If they all pass, then you still need to exercise care and watch for unexpected results as you read it.

Now, given the **KRESV** tests, imagine that you want to send email with an attachment to someone with whom you've never corresponded – what should you do? Here's a set of steps to follow to begin an email dialogue with someone.

Since the recipient doesn't already **Know** you, you need to send them an introductory email. It must not contain an attachment. Basically, you're introducing yourself and asking their permission to send email with an attachment that they may otherwise be suspicious of. Tell them who you are, what you'd like to do, and ask for permission to continue.

This introductory email qualifies as the mail **Received** from you.

Hopefully, they'll respond; and if they do, honor their wishes. If they choose not to receive email with an attachment from you, don't send one. If you never hear from them, try your introductory email one more time.

If they accept your offer to receive email with an attachment, send it off. They will **Know** you and will have **Received** email from you before. They will also **Expect** this email with an attachment, so you've satisfied the first three requirements of the **KRESV** tests.

Whatever you send should make **Sense** to them. Don't use a provocative Subject line or any other social engineering practice to encourage them to read your email.

Check the attachments for **Viruses**. This is again based on having virus-checking programs,

The **KRESV** tests help you focus on the most important issues when sending and receiving email with attachments. Use it every time you send email, but be aware that there is no full proof scheme for working with email or security in general. You still need to exercise care. While an anti-virus program alerts you to many viruses that may find their way to your computer, there will always be a lag between when a virus is discovered and when anti-virus program vendors provide the new virus signature. This means that you shouldn't rely entirely on your anti-virus programs. You must continue to exercise care when reading email.

Virus warning: Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users. Action to take is contact your manager or the City of Detroit Help Desk and assistance will be supplied

III. Exception:

The City Information Technology Services Director and City Corporation Counsel must approve any exceptions to this policy

IV. Approval Block

Email Usage Policy	
Approval Date: 1/10/2014	**Review: Bi-Annual**
Effective Date: 1/10/2014	**Last Review = 3/1/2016**