City of Boston	Information Technology Policies & Procedures	
	Policy Title: Information Technology Resource Use Policy	Platform: All
	Date of Approval: 01/21/2015	Version No. 2

Information Technology Resource Use Policy

The City of Boston recognizes the importance of modern technology and access to information in providing citizens the best and most efficient services. Therefore, the City has given many of its employees and contracting personnel e-mail accounts and access to the Internet.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, PDA's, network accounts, e-mail accounts, web browsing, blogging, Web2.0, social networking, and FTP (i.e. "Information Technology Resources") provided by the City, are, and at all times remain, the property of the City of Boston. Access and use of these systems and equipment is solely for business related purposes.

This policy outlines the acceptable use of computer equipment, e-mail, and Internet related resources and services at the City, i.e. Information Technology Resources. These rules are in place to protect the employees and the City. Inappropriate use of Information Technology Resources exposes the City to liability and risks, including, virus attacks, compromise of network systems and services, and potential litigation.

Note: If printed, content is valid only for the day it was printed. Always refer to **The Hub – Document Library** for the current version. If the user elects to maintain copies of this policy or procedure, it is their responsibility to verify the currency of the document by checking it against the online version. This document must be promptly removed from use when obsolete

1.0 APPLICABILITY

1.1. This policy applies to all employees and affiliates including contractors, consultants, vendors, etc. at the City who are granted access to equipment, software, networks, etc. that is owned, leased, and/or operated/maintained by the City of Boston. These individuals will be known and referred to as "User(s)."

1.2. Access and/or use of Information Technology Resources constitutes the user's acknowledgement and consent to this policy as well as his/her consent to the City's recording and monitoring of his/her use (whether for personal or business purposes) of Information Technology Resources.

1.3. This policy is not intended to list all forms of acceptable and unacceptable use. Employees have the responsibility to use Information Technology Resources in an efficient, effective and lawful manner. Users must follow the same code of conduct expected in any other form of written or face-to-face business communication. The City may supplement or modify this policy for employees in certain roles. This policy combines and supersedes the City's *Acceptable Use Policy*, *Email Use Policy*, and *Internet Use Policy*.

2.0 DEFINITIONS

2.1. BLOGGING - An online journal that is frequently updated and intended for general public consumption.

2.2. E-MAIL - The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical e-mail clients include Microsoft Outlook.

2.3. CHAIN E-MAIL - E-mail sent to successive people. Typically, the body of the note has directions to the reader to send out multiple copies of the note so that good luck or money will follow.

2.4. FORWARDED E-MAIL - E-mail resent from a network to another point.

2.5. EMPLOYEE - Any individual employed by the City of Boston or its affiliated agencies or departments in any capacity, whether full or part-time, active or inactive, including interns, contractors, consultants and vendors.

2.6. ENCRYPTION - The translation of data into a secret code to achieve data security.

2.7. HACKING SITES - Web sites which provide content about breaking or subverting computer security controls.

2.8. INFORMATION TECHNOLOGY RESOURCES - Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, PDA's, network accounts, e-mail accounts, web browsing, blogging, Web2.0, social networking, and FTP provided by the City to authorized users to facilitate the completion of their jobs.

2.9. INSTANT MESSAGING - A type of communications service that enables the creation of a kind of private chat room with another individual in order to communicate in real time over the Internet.

2.10. INTERNET RESOURCES - Web sites, instant messaging applications, file transfer, file sharing, and any and all other Internet applications and activities using either standard or proprietary network protocols. Examples of web sites that pose a risk to the City of Boston or counter to its mission are malware repositories, sites advocating violence against civil society or against persons based on race, religion, ethnicity, sex, sexual orientation, color, creed or any other protected categories; sites offering gambling activities or that are pornographic in nature.

2.11. IP ADDRESS - Unique network address assigned to each computing device connected to a network to allow it to communicate with other devices on the network or Internet.

2.12. MALWARE - Malware is any software, application, program, email or other data or executable code which is designed to cause harm to a network or computer or violate any law, statute, policy or regulation in any way. Examples of harmful activity or intent are theft of personal information or intellectual property by phishing or other means, hacking, violation of copyright law (distributing or copying copy written material without proper authorization), propagation of Spam e-mails, harassment, extortion, denial of service and facilitating access to illegal content (pornography, gambling, etc.). Accessing or storing malware is expressly prohibited unless authorized for research or forensic purposes by appropriately authorized and designated employees.

2.13. NETWORK - Any and all network and telecommunications equipment, whether wired or wireless, controlled or owned by the City of Boston which facilitate connecting to the Internet.

2.14. PHISHING - Attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

2.15. SENSITIVE INFORMATION - Classified as Protected Health Information (PHI), Confidential Information or Internal Information.

2.16. SPAM - Unsolicited nuisance Internet E-mail which sometimes contains malicious attachments or links to web sites with harmful or objectionable content.

2.17. SPOOFING - The act of replacing IP address information in an IP packet with falsified network address information. Each IP packet contains the originating and destination IP addresses. By replacing the true originating IP address with a falsified address a hacker can obscure their network address and hence the source of a network attack making traceability of illegal or illegitimate internet activity extremely difficult.

2.18. UNAUTHORIZED DISCLOSURE - The intentional or unintentionally act of revealing restricted information to people, both inside and/or outside the City, who do not have a need to know that information.

2.19. USER(S) - Individual(s) whether full or part-time, active or inactive, including interns, contractors, consultants, vendors, etc. who have been given access to and granted permission(s) to use Information Technology Resources.

2.20. USER ID - Uniquely assigned Username or other identifier used by an employee to access the City of Boston network and systems.

2.21. VIRUS WARNING - E-mail containing warnings about virus or malware. The overwhelming majority of these e-mails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

3.0 POLICY

3.1. Acceptable Use: City of Boston employees are only permitted to use Information Technology Resources for purposes which are safe (pose no risk to employees or assets), legal, ethical, do not conflict with their duties or the mission of the City of Boston and are compliant with all other City of Boston policies. Usage that meets the aforementioned requirements is deemed “proper” and “acceptable” unless specifically excluded by this policy or other City of Boston policies.

3.2. Unacceptable Use: Unless such use is reasonably related to a user’s job, it is unacceptable for any person to use Information Technology Resources for:

3.2.1. the purpose of gambling/gaming or engaging in any illegal activity;

3.2.2. any commercial purpose;

3.2.3. the transmission of confidential information to unauthorized recipients;

3.2.4. viewing, downloading, or transmitting sexually explicit, obscene or otherwise pornographic materials;

3.2.5. the creation or distribution of chain emails, any disruptive or offensive messages, offensive comments about race, gender, disabilities, age, sexual orientation, gender identity or expression, religious beliefs/practices, political beliefs, or material that is in violation of workplace harassment or workplace violence laws or policies;

3.2.6. infringement of any intellectual property rights;

3.2.7. disabling any and all antivirus software or other security controls running on or used by Information Technology Resources;

3.2.8. significant consumption of City network and system resources for non-business related activities (such as video, audio or downloading large files) or excessive time spent using Information Technology Resources for non-business purposes (e.g. shopping, social networking, sports related sites, et al).

3.3. Personal Use: Information Technology Resources are provided solely for the conduct of City business. However, the City realizes and is aware of the large role technology (especially the Internet and email) plays in the daily lives of individuals. In this context, the City acknowledges that a limited amount of personal use of Information Technology Resources is acceptable. This use must not interfere with the user's job responsibilities; it cannot involve any activities expressly prohibited by this or any other City policy; and it should be limited to designated break periods and/or the user's lunch break.

3.4. Accountability: Users are prohibited from anonymous usage of Information Technology Resources. In practice, this means users must sign in with their uniquely assigned City of Boston User ID before accessing/using Information Technology Resources. Similarly, "spoofing" or otherwise modifying or obscuring a user's IP Address or any other user's IP Address is prohibited. Circumventing user authentication or security of any host, network, or account is also prohibited.

3.5. Passwords: In addition, users are prohibited from revealing or sharing their account password(s) with anyone including colleagues, superiors, friends, family, etc. (For further information regarding passwords, see the *Password Policy*.) Allowing the use of your account by another user is also strictly prohibited.

3.6. Public Records: All users are advised that their use of Information Technology Resources, including Email, may result in the creation of Public Records; and it is the user's responsibility to properly manage and maintain such records. There are three categories of email messages: (1) Junk Mail, SPAM, and personal messages are not public records and should be deleted immediately. (2) Transitory records should be deleted once their use ceases. (3) Public Records should be retained according to schedule. For further information regarding the management and retention of Public Records, see the Archives Division's *General Records Retention Policy* and *Email Management and Retention Policy*.

3.7. **Enforcement**

3.7.1. Record of Activity: User activity with Information Technology Resources may be logged. Usage may be monitored or researched in the event of suspected improper Information Technology Resource usage or policy violations.

3.7.2. Blocked or Restricted Access: User access to specific Internet resources, or categories of Internet resources, deemed inappropriate or non-compliant with this policy may be blocked or restricted. A particular web site that is deemed "Acceptable" for use may still be judged a risk to the City (e.g. it could be hosting malware), in which case it may also be subject to blocking or restriction.

3.7.3. Privacy: Users have no expectation of privacy regarding their use of Information Technology Resources. Log files, audit trails and other data about user activities with Information Technology Resources may be used for forensic training or research purposes, or as evidence in a legal or disciplinary matter.

3.7.4. Consequence of Policy Violation: Users found to be in violation of this policy may be subject to discipline up to and including termination. The concept of progressive discipline will apply except in serious cases.

3.8. The City of Boston reserves the right to review any usage and make a case-by-case

determination whether the user's duties require access to and / or use of information technology resources which may not conform to the terms of this policy.

4.0 ROLES AND RESPONSIBILITIES

4.1. Users: are responsible for their own use of Information Technology Resources and are advised to exercise common sense and follow this policy (i.e. "Information Technology Resource Use Policy") in regards to what constitutes appropriate use of Information Technology Resources in the absence of specific guidance.

4.2. Chief Information Security Officer: is responsible for monitoring compliance with this policy.

5.0 RELATED INFORMATION

5.1. Mobile Device Policy
5.2. Bring Your Own Device (BYOD) Policy
5.3. Password Policy
5.4. Social Media Policy
5.5. City Clerk Archives Division, General Records Retention Policy
5.6. City Clerk Archives Division, Email Management and Retention Policy

6.0 SUPPORT CONTACT

6.1. DoIT Service Desk, 617-635-7378, DOITservicedesk@boston.gov

7.0 RETENTION

The City of Boston Department of Innovation & Technology will retain this policy and review it on an annual basis to ensure that it remains effective, complies with internal operational parameters, meets identified City of Boston business goals and industry best practices.

8.0 REVISION HISTORY

Date	Rev. No.	Change	Ref. Section(s)	Person(s) Responsible
4/1/2011	1.0	First version	All	Bryce Cunningham
1/20/2015	2.0	Revision	All	Greg McCarthy

9.0 Approval List:

Title:	**Name:**	**Date:**
Document Owner	IT Security Team	January 20, 2015
Preliminary Approver	Dan Rothman, CTO	January 21, 2015
Final Approver	Jascha Franklin-Hodge, CIO	January 21, 2015