



CITY OF HOUSTON

Administrative Procedure

Subject: **Use of City Information and City Information Technology Resources**

A.P. No:

8-1

Effective Date:

October 17, 2014

1. AUTHORITY

1.1 Article VI, Section 7a, of the City Charter of the City of Houston.

2. PURPOSE

2.1 This document establishes a City-wide policy for appropriate use, access, and maintenance of the integrity of City information and City information technology (IT) resources, regardless of the physical location of the resource and information.

3. BACKGROUND

3.1 The City is the trusted custodian of employee, citizen, government and business information. The City protects and ensures the confidentiality, integrity, and availability of all its information and IT resources, regardless of how they are created, distributed, or stored.

3.2 The City implemented security controls to protect all information assets (including hardware, systems, software, and data) and to ensure compliance with all laws.

3.3 It serves the interests of the City to enhance the quality of the workplace, create a supportive workplace, and promote work-life balance. Thus, the City will permit employees to address important personal matters during lunches and breaks when such matters cannot be addressed easily outside of work hours, as long as such activities: are conducted in a responsible, limited manner; comply with the City's IT security policies, and applicable laws; involve minimal expense to the City; do not interfere with conducting City business; and preserve the public trust.

4. OBJECTIVES

4.1 To maintain compliance with applicable laws governing City information and the City IT resources on which City information resides or is stored.

4.2 To ensure that access to, and use of, City information and City IT resources complies with applicable laws or City policy, such as laws pertaining to sensitive information.

4.3 To safeguard the confidentiality, integrity, and availability of City information and City IT resources, through the establishment of reasonable physical and technological security measures, policies, and standards.

4.4 To establish policies and standards regarding the protection and sanitization of City information, including Sensitive Information that resides or may reside on any City IT resource or City-owned mobile device.

Approved:

Handwritten signature of Cynthia D. Parker in black ink.

Date Approved:

10/17/2014

Page 1 of 15

- 4.5 To manage and minimize risks and liabilities to the City, the City's employees, and citizens, which could result from theft, damage, loss, and improper or unauthorized use or disclosure of City information and City IT resources.
- 4.6 To provide examples of acceptable and prohibited uses and activities involving City information and City IT resources.
- 4.7 To inform users of their responsibilities involving City information and City IT resources and to manage users' privacy expectations when using City IT resources or creating, storing, or accessing City information.

5. SCOPE

- 5.1 All City departments and divisions are required to adhere to this policy.
- 5.2 This policy applies to any party who is granted access, accesses, uses, or connects to City IT resources to conduct City business.
- 5.3 This policy applies to all of the following persons who use City IT resources to conduct City business: City employees, City officials, Mayoral appointees (boards, commissions, and authorities), vendors, contractors, independent contractors, consultants, interns, temporary employees, volunteers, users, or their guests.
- 5.4 This policy governs user conduct in connection with engaging in City business regardless of where it occurs, whether through network connections, wireless connections, or remote access.
- 5.5 This policy governs all City information, regardless of where it exists, resides, is stored, accessed, processed, or maintained.
- 5.6 The use of public-facing resources is excluded from the scope of this policy, except where users conduct City business or access City information or City IT resources using public-facing resources.
- 5.7 Unless otherwise stated in this policy, personally-owned IT resources and mobile devices and the use of such personal IT resources and mobile devices are excluded from the scope of this policy.
- 5.8 This policy does not list all forms of acceptable and unacceptable uses or activities, nor does it detail all of the standards applicable to each subpart contained herein. Use of and access to City information and City IT resources is a privilege, not a right. The City may revoke or limit this privilege at any time which may result in conditions that jeopardize the user's ability to perform required work functions and disciplinary actions. Users are responsible for and expected to use good judgment and reasonable care in protecting and accessing City information and City IT resources. Users are responsible for accessing and using all City information and City IT resources in a safe, ethical, professional, and lawful manner.
- 5.9 This policy covers the following areas:
 - 5.9.1 Acceptable Use
 - 5.9.2 Internet and Email Communications
 - 5.9.3 Software License Compliance

6. DEFINITIONS

City Business – Any action, work, or function authorized to perform by any person on behalf of the City or in connection with conducting or transacting business for or with the City. City business includes any one or more of the following activities: (i) transacting or engaging in any official business as that term is defined by Texas Government Code Section 552.003(2-a), as amended from time to time; (ii) connecting to the City’s IT resources to read or send email, access and view Intranet web resources, perform system and administrative functions, and download or store City information; and (iii) performing work where the City’s Information may be created, transmitted, or stored on a City-owned mobile device.

City Employee – Any person who receives compensation as an employee of the City, including interns, temporary employees and other personnel, regardless of civil service status, classification, contract employee status, pay grade, or full-time or part-time status.

City Official – Has the meaning defined in Section 18-2 of the City Code of Ordinances, as amended from time to time.

City Information – Any Electronically Stored Information (ESI) that is written, created, produced, collected, assembled, or maintained under a law or ordinance or in connection with the transaction of City business, including any Sensitive Information or Confidential Information, and any data or information created on, stored on, residing in, processed by, transmitted to, received by, maintained by, or accessed using the City’s IT resources, including City-owned mobile devices. City information also includes any public information, in electronic form, as defined in Section 552.002 of the Texas Government Code, as amended from time to time.

City-owned Mobile Device – Any mobile device or wireless communication device provided by, owned by, or wholly paid for by the City.

City IT Resources – Any IT resource or a collection of IT resources that are used, owned, leased, operated, managed, controlled by, or in the custody of the City. City IT resources includes software that the City purchases, licenses, subscribes to, installs, or develops; City-owned mobile devices; City-published websites and software; IT resources the City provides to users to facilitate accomplishing City business, and City IT Asset as defined in Administrative Procedure 8-3, Managing IT Policy Exceptions Policy. IT resources includes all systems, hardware, software, equipment, supporting infrastructure, and the data contained in, stored on, or processed by any of these resources, including computers, websites and FTP sites, databases, applications, apps, mobile devices, storage media, printers, scanners, fax machines, telecommunications equipment and devices, voice and data systems, Internet, Intranet, email, social networking, user and network accounts, and all associated processes, services, and data.

Confidential Information – Any information defined by law as confidential, including Sensitive Information and information that is exempt from public disclosure under the Texas Public Information Act (TPIA) or other applicable laws.

Contractor – Has the meaning defined in Section 18-2 of the City Code, as amended from time to time.

Discovery – Refers to the process of identifying, locating, collecting, reviewing, and producing ESI, documents, and data for use in the context of the legal process, such as in litigation or responding to subpoenas or investigations.

Electronically Stored Information (ESI) – Any information, document, file, or data that is in electronic form or that is created, received, maintained, stored, or residing on any IT resource, removable media, or mobile device. ESI includes documents, correspondence, emails, calendar entries, notes, metadata, spreadsheets, databases, video and audio files, images, text messages,

instant messages, messages transmitted using systems proprietary to the mobile device manufacturer (e.g. iMessage or Blackberry messenger), social media communications (e.g. posts on FaceBook, LinkedIn, or other social media sites), voicemails, logs, blogs and microblogs, browser history, cached files, audit trails, web pages, and other similar electronic information. ESI also includes any information stored in or accessible through a computer or other information retrieval system or device, including any database, ESI contained in the database and machine-readable materials.

Encryption – Refers to the translation of data into a secret code to achieve data security. Access to a secret key or password is necessary to read or decrypt an encrypted file.

Jailbroken Devices – A device which has been tampered with or modified such that limitations imposed by the device manufacturer have been removed.

Law(s) – Refers collectively to all laws, statutes, ordinances, rules, regulations, policies, and other types of local, state, national and foreign government authority, including the City Charter, City of Houston Code of Ordinances, case law, common law, and other laws applicable to this policy.

Malware – Any software, application, program, email, or other data or code that is designed to cause harm to an IT resource or to violate any law in any way. Malware includes a variety of hostile, intrusive, or annoying software or program code, such as viruses, worms, Trojan horses, rootkits, and spyware.

Mobile Device – Any device that can be carried by a person or is generally intended to be portable and the device is capable of containing or storing data, even temporarily. Mobile devices includes portable computers, laptops, notepads, tablet PCs, tablets, smartphones, wireless communication devices, cell phones, pagers, personal digital assistants (“PDAs”), Blackberry© devices, Bluetooth© devices, digital cameras, removable media, and any other similar portable computing and/or communication devices. Unless otherwise specifically stated, all references in this policy to mobile devices, regardless of ownership, refers to mobile devices that are used, in whole or in part, in connection with conducting City business, including mobile devices that are used to access City information or City IT resources, or mobile devices on which City information is maintained, stored, or resides.

Mobile Device Management (MDM) – Software or other technology systems that manage the security controls, certain functionality, and connectivity of mobile devices attempting to connect to the City’s IT resources. MDM software enables the City to enforce policies and to configure, secure, monitor, and remotely wipe mobile devices.

Monitoring Efforts – Has the meaning defined in Section 8 of this policy.

Network – Refers to the sub-category of IT resources, whether wired or wireless, that are linked together to facilitate a connection, communication, exchange, or sharing among or between users or other IT resources. Network includes telecommunications equipment and other connections to or between the Internet, Intranet, or other computers, workstations, and IT resources.

Peer-to-Peer (P2P) Communications – Networks, systems, applications, or IT resources that allow users connected to the Internet to link or share their computers with another user’s computer or to transform the user’s computer into a server for the purpose of finding, sharing, uploading, downloading, or retrieving files.

Personal or Personally – When used in connection with any IT resource, mobile device, or software, “personal” or “personally” refers to any IT resource, mobile device, user account, or software paid for (whether in whole or in part), owned, leased, or issued by any person or entity other than the City, third-party tools, websites, or apps designed for sharing, collaboration, or storage such as Dropbox©.

Public-Facing Resource – The City’s web pages, social media sites, and City IT resources that the City intends for the general public to access or use, such as the Houston Public Library, or computers provided by the City at locations where payments due to the City are accepted.

Removable Media – Any storage media or device, which can be removed from its reader device, conferring portability to the data the storage media device carries. Removable media includes CDs, DVDs, thumb drives, USB drives, external hard drives, memory cards or sticks, diskettes, tapes, and other similar devices.

Remote Access – The ability to get access to a physical City IT resource from a remote distance or non-City location, including through the use of a modem, virtual private network (VPN), or wireless activity.

Sensitive Information – Information deemed by the City or by law to be sensitive in nature and merits limited access and special precautions to protect the information from inappropriate or unauthorized use, access, disclosure, modification, loss, or deletion. Sensitive Information may be public, confidential, or personally identifiable information. Sensitive Information may include credit card numbers, social security numbers, driver’s license numbers, date and place of birth, financial information, criminal or employment history, sensitive security information as defined by 49 C.F.R. § 1520.5, as amended from time to time, protected health information, information that would violate an individual’s privacy rights if disclosed, information protected by non-disclosure obligations, and information protected from disclosure under the TPIA, Section 552 of the Texas Government Code, as amended from time to time.

Tablet – Refers to an open-face wireless device or other wireless communication device with a touchscreen display and without physical keyboards. Examples of tablets include iPads, Kindles, Nooks, Samsung Galaxies, Microsoft Surfaces, HP ElitePads, and e-readers.

User – Any person who is granted access, accesses, uses, or connects to City IT resources to transact City business. User also includes a person who is granted access, accesses, uses, or connects to a public-facing resource to transact City business or to connect to or access City IT resources or City information. User includes all City employees, City officials, Mayoral appointees (boards, commissions, and authorities), vendors, contractors, independent contractors, consultants, volunteers, and their guests who access, use, or connect to City IT resources in connection with conducting City business.

User ID – The unique user name, log-in, or other identifier used to identify a user and to allow access to an IT resource.

7. USER PRIVACY

- 7.1 All City information and City IT resources are the property of the City, including all City information created or generated by, accessed from, backed up, or stored on City-owned mobile devices and personal IT resources.
- 7.2 Users have no expectation of privacy, confidentiality, or anonymity while using or accessing City IT resources and City information unless the information regarding the user’s activities or identity is specifically protected by law from disclosure and then only to the extent of that legal protection. The City’s provision of IT resources and requirements to use a user ID and password do not imply any expectation of privacy, confidentiality, or anonymity for the user nor do they imply an exclusion from monitoring efforts.
- 7.3 There should be no expectation of privacy, anonymity, or confidentiality regarding any of the user’s activities and the data below, which data remains the property of the City:

- 7.3.1 User's access to City information or use of City IT resources, including City-owned mobile devices;
 - 7.3.2 Any data and ESI that users generate, create, store, send, forward, backup, or receive in connection with conducting City business or using City IT resources; and
 - 7.3.3 Any files, emails, or other ESI maintained by, generated by, or stored on City IT resources and City-owned mobile devices.
- 7.4 The City may, at its discretion, conduct monitoring efforts in furtherance of any lawful purpose at any time and without further notice to the user. The City may, at its discretion or as otherwise required by law, disclose information, which may include identification information about the user, to appropriate third parties, including law enforcement officials.

8. MONITORING

- 8.1 In accordance with City policies and applicable laws, the City has the right to and may, at any time, research, monitor, collect, log, audit, inspect, intercept, record, read, search, seize, and copy all aspects of City information and City IT resources, without any further notice to users (collectively "monitoring efforts"). Monitoring efforts involving City IT resources may include any one or more of the following efforts:
- 8.1.1 Maintaining and reviewing logs, log files, and audit trails of users' activities;
 - 8.1.2 Monitoring users use of or access to ESI provided by or through the City, including personal data on City-owned mobile devices;
 - 8.1.3 Auditing and inspecting City IT resources, including computers and networks, for illegal software or unacceptable use of City IT resources; and
 - 8.1.4 Collecting and monitoring location or GPS tracking information that may be obtained as part of the normal management of the City IT resource in any one or more of the following limited circumstances:
 - 8.1.4.1 To monitor City employees, whose City IT resources and City-owned mobile devices may be used explicitly for the purpose of location tracking, real-time-location-based dispatch, and other location-based business functions and tasks, such as tracking data created and monitored in providing City services for City employees or the public, including services related to emergencies and public safety, transportation, waste management, public utilities, fleet management, and couriers;
 - 8.1.4.2 To locate the City IT resource if it is lost or stolen;
 - 8.1.4.3 When the user expressly consents or requests that the City collect, monitor, track, or reveal the City IT resource's location;
 - 8.1.4.4 To assist a user in distress or a user who is believed to be in distress; and
 - 8.1.4.5 When a governing body with jurisdiction compels the City to collect, monitor, or track the City IT resource or to produce any such information to the extent it was obtained in the normal management of the resource.

- 8.2 Monitoring efforts involving Houston Police Department (HPD) or Houston Airport System (HAS) employees, internal networks, and systems shall be conducted by HPD or HAS, respectively, or if specifically authorized by the Chief of Police or the Director of HAS, or their designees.
- 8.3 Information and data subject to monitoring efforts also include all information contained in or transmitted using City IT resources, as well as the contents and related transmissions using any City-owned mobile devices, including files, downloads, call logs, text messages, emails, digital photos, Internet browser history, Internet usage, and data access. Because City information and City IT resources are City property, the City is not required to provide notification to or seek permission from users or other persons to conduct monitoring efforts. The absence of monitoring efforts in any specific situation does not constitute a waiver of the City's right to conduct monitoring efforts.
- 8.4 The City may engage in monitoring efforts in connection with City IT resources and City information where such efforts are conducted by authorized City personnel for lawful purposes. For example, authorized monitoring efforts may occur in furtherance of any one or more of the following purposes:
- 8.4.1 Providing information and data in response to a request or requirement (a) under the TPIA, a court order, or any applicable law or policy; (b) relating or pursuant to discovery, any civil investigative demand, investigation, or a legal or disciplinary matter; or (c) issued by a regulatory agency or other governmental body;
 - 8.4.2 Complying with the City's document management and data retention policies;
 - 8.4.3 Investigating functionality or performance of City IT resources;
 - 8.4.4 Reviewing user's usage and compliance with this policy and other laws, including investigating alleged violations of any City policies or laws;
 - 8.4.5 Ensuring the integrity and protection of City information and City IT resources, including conducting security audits and forensic analysis;
 - 8.4.6 Investigating, detecting, and protecting against suspicion of criminal activities, fraud, unauthorized use or disclosure, improper use, abuse, security threats, vulnerabilities, or breaches; and
 - 8.4.7 For any other lawful purposes, including any legitimate business, legal, or disciplinary purpose.
- 8.5 In the event that the City becomes aware of any prohibited uses, the City will respond in a timely and appropriate manner as the circumstances warrant, including disconnecting or suspending access to City information and City IT resources. The City may, at its discretion or when required by law, disclose information discovered during monitoring efforts to authorized personnel and law enforcement officials for various purposes, including criminal, civil, and administrative investigations.
- 8.6 Monitoring efforts may result in disciplinary or remedial actions taken against the user, including financial liability, disciplinary action up to and including indefinite suspension/termination of employment, loss of use, termination of contractual agreements with contractors, denial of or restricted access, criminal and civil penalties, and any other action deemed appropriate by the City.

8.7 In accordance with City policies and without further notice to users:

- 8.7.1 Department Directors, the Office of the Inspector General, authorized personnel from Human Resources and the Legal Department, HAS, and HPD may conduct monitoring efforts in furtherance of their normal job responsibilities, provided that these personnel obtain the necessary, written authorization. Houston Information Technology Services (HITS) and department IT personnel are permitted to provide technical assistance upon request in furtherance of authorized monitoring efforts described in this paragraph.
- 8.7.2 Authorized IT personnel may, at any time, conduct monitoring efforts, provided such efforts comply with the applicable laws and City policies and are conducted solely for security, operational, support, and maintenance purposes.
- 8.7.3 Unauthorized monitoring efforts violate this policy and may violate City policies and other laws.

9. ACCEPTABLE USE

9.1 ALLOWED USES:

- 9.1.1 City IT resources are intended primarily for uses in connection with conducting City business.
- 9.1.2 Users are permitted to use City information and City IT resources only for purposes that are safe, legal, ethical, do not conflict with the user's duties and is compliant with all other laws. Usage that meets all of these requirements are deemed "proper", "allowed," and "acceptable" (which terms are used interchangeably) unless specifically excluded by City policies.
- 9.1.3 Limited personal use of City IT resources to conduct non-City business may be permissible when the use is authorized by management, incidental, and it occurs occasionally during the City employee's working hours (collectively "Allowed Personal Uses"), as long as the allowed personal uses do not involve any one or more of the following characteristics:
 - 9.1.3.1 Cause or lead to any additional expense to the City;
 - 9.1.3.2 Negatively impact overall employee productivity;
 - 9.1.3.3 Interfere with the normal operations of the City employee's department, work unit, or the City IT resource;
 - 9.1.3.4 Compromise the City, City information, or City IT resources in any way; and
 - 9.1.3.5 Violate any other elements of this policy, any law or other City policies.

9.2 PROHIBITED USE: The following list of activities and uses of City information and City IT resources (collectively "Prohibited Uses") are strictly prohibited at any time by any user, unless performed (a) for law enforcement purposes; (b) by the Office of Inspector General, the Legal Department, or Human Resources in the course of legitimate job responsibilities; or (c) for other lawful purposes as expressly authorized in writing by a department director or designee. The list below is not exhaustive, but merely provides a framework for activities that fall into categories of Prohibited Uses.

- 9.2.1 Engaging in any activity that violates any law or City policies, including City policies regarding appropriate activities in the workplace and Executive Order 1-18, Policy on Use of Social Media;
- 9.2.2 Intentionally creating, accessing, downloading, viewing, storing, or transmitting sexually explicit or sexually-oriented materials. This prohibition does not apply to video or audio files created as part of authorized surveillance or monitoring services, where the video or audio files incidentally record or contain persons engaging in sexually explicit acts;
- 9.2.3 Engaging in any activity that violates Executive Order 1-50, the City's Workplace Discrimination and Harassment policy, as amended from time to time, including the creation or transmission of any materials that ridicule, harass, or discriminate on the basis set forth in the executive order;
- 9.2.4 Intentionally creating, accessing, or transmitting materials that contain offensive, threatening, or disruptive content, including any text or image that can be considered racially offensive, defamatory, disparaging, obscene, hate speech, or otherwise violating the legal rights of others;
- 9.2.5 Intentionally creating, accessing, downloading, viewing, storing, copying, or transmitting materials related to illegal weapons and terrorist activities;
- 9.2.6 Intentionally and knowingly causing security breaches or engaging in activities that would compromise the security of or harm any City information or City IT resources. This includes intentionally and knowingly avoiding, disabling, or circumventing City-established security procedures and controls; sharing or disclosing a person's user ID or other means of digital authentication (including passwords) without authorization; jail breaking a City-owned mobile device or using a jailbroken device to conduct City business; or introducing, uploading, downloading, or distributing malware;
- 9.2.7 Intentionally and knowingly storing Sensitive Information on an unauthorized device;
- 9.2.8 Intentionally and knowingly using City information and City IT resources in any manner that may damage, impair, disrupt, or interfere with the City's IT resources;
- 9.2.9 Intentionally attempting to gain unauthorized access to any City information and City IT resources through hacking, password cracking, using a password and user ID other than the one the user is assigned or authorized to use, or through any other unlawful or unethical means;
- 9.2.10 Accessing, downloading, reading, deleting, copying, modifying, printing, or transmitting another user's data, user ID, identification, password, or ESI without proper authorization;
- 9.2.11 Restricting, inhibiting, or preventing another user from accessing or using City information and City IT resources without proper authorization;
- 9.2.12 Using City IT resources to gain unauthorized access to other IT resources;
- 9.2.13 Impersonating another user or representing oneself as someone else including either a fictional or real person;

- 9.2.14 Using P2P communications that have not been purchased by the City for use in conducting City business or have not been approved by the Chief Information Officer (CIO);
- 9.2.15 Creating or using unauthorized distribution lists in the City-provided email system or distributing unauthorized newsletters or other publications using the City-provided email system or a City email account;
- 9.2.16 Distributing anonymous email messages, such as email messages where the recipient is unable to view the sender's name or email address, or the use of an email tool or service that conceals the originator of the email message;
- 9.2.17 Creating, copying, transmitting, or forwarding chain letters, junk email, or other unauthorized mass mailings regardless of the subject matter;
- 9.2.18 Accessing, disclosing, or transmitting Confidential Information to unauthorized recipients or failing to secure the transmission of or access to Confidential Information in compliance with City policies, including the use of DropBox or other data storage repositories unless such use is authorized by City policies or approved, in writing, by appropriate IT personnel;
- 9.2.19 Acquiring, using, reproducing, copying, transmitting, distributing, downloading, or reproducing materials, images, audio or video files, software, or any other document or ESI that is protected by copyright, trademark, license or other intellectual property and legal rights without proper authorization. The user is responsible for obtaining the proper authorization and the City assumes no responsibility for a user's failure to obtain this proper authorization;
- 9.2.20 Downloading or installing software, freeware/shareware or executable program files from the Internet or other electronic sources to City IT resources without approval from the appropriate IT personnel. This includes games, scanners, password crackers, anti-malware software, firewalls, and web browsers.
- 9.2.21 Adding, downloading, installing, or connecting personal IT resources to City IT resources without the appropriate management authorization, including the installation of modems on City data lines, home computers, and reconfiguration of systems. This prohibition does not apply to commonly used and secure personal IT resources, such as software necessary to enable printing (e.g. printer drivers and related software) or other software that facilitates the City employee's performance of his/her job responsibilities;
- 9.2.22 Using the City's IT resources to establish personal, commercial, and/or non-profit organizational web pages;
- 9.2.23 Using City IT resources for commercial purposes, private gain, in support of "for-profit" activities, or in support of other outside employment or business activity (such as consulting for pay, sales or administration of business transactions, or sale of goods or services);
- 9.2.24 Creating, soliciting, or transmitting campaign materials or materials in connection with political, religious, charitable, fund-raising, or other non-City business activities that are not authorized by the appropriate City personnel;

- 9.2.25 Consuming a significant amount of City IT resources or accessing non-business related applications or websites that maintain a persistent connection to the Internet for non-City business related purposes (such as streaming audio and video, or downloading large files). Consumption of a significant amount of City IT resources for non-City business related purposes occurs when the consumption (a) materially reduces the functionality of, interferes with, or disrupts the performance or operation of the City IT resource; (b) interrupts or interferes with City business; or (c) decreases the user's productivity in conducting City business during the user's work hours;
- 9.2.26 Engaging in gambling or on-line gaming;
- 9.2.27 Engaging in any personal use that does not qualify as allowed personal use under this policy as defined in section 9.1.3 such as spending excessive time using City IT resources for non-City business purposes (e.g. shopping, checking personal email accounts, or visiting social networking sites); and
- 9.2.28 Using City information and City IT resources for any other purpose outside of the acceptable uses authorized by this policy and other City policies.

- 9.3 Department directors may enact departmental policies that exceed the requirements stated in this section.
- 9.4 Employees are encouraged to seek assistance in advance from management and Human Resources to determine whether a use is for City business purposes, personal, prohibited, or allowed, and whether the personal uses are incidental.
- 9.5 The City accepts no responsibility for any uses, activities, or Internet traffic that violate this policy or the acceptable use policy of any third party's network or IT resource that is connected to a City IT resource, either directly or indirectly, except that, to the extent feasible, the City may notify the City employee that the City employee is alleged to be in violation of a third party's acceptable use policy if the third party so notifies the City, in writing, and provides the City with sufficient information for the City to identify the specific City employee alleged to have violated the third party's acceptable use policy.

10. INTERNET AND EMAIL COMMUNICATIONS

- 10.1 The City provides email, Intranet, and Internet access as a City IT resource, where necessary, for City employees to conduct City business. Users access to and use of City email and the Internet is a privilege that the City may wholly or partially revoke, at its discretion, without notice or consent of the user.
- 10.2 City Internet, Intranet, and email resources, including emails sent or received using City email, are the property of the City.
- 10.3 When users access the Internet using Internet addresses and domain names registered to the City, they may be perceived by others to represent the City. Thus, when accessing the Internet using the City's Internet address, IP addresses, or domain name registered to or associated with the City, users shall not use the Internet for any purpose which would reflect negatively on the City or its employees.
- 10.4 Users should exercise reasonable caution to protect the contents of City Information and email communications, including encrypting the contents of email by using City-owned encryption technology, where appropriate, or where encryption is otherwise required by contract, City policy, or by law, such as laws pertaining to Sensitive Information.

11. SOFTWARE LICENSE COMPLIANCE

- 11.1 Users shall not install on City IT resources any software that lacks an appropriate license. The only software authorized for use on City IT resources is software that has been (a) purchased through the normal City requisition procedures, (b) made available to the City for a trial period in accordance with applicable City requisition and procurement procedures, (c) approved by appropriate City personnel; or (d) other limited, personally-owned software that is exempted from the Prohibited Use restrictions in this policy.
- 11.2 Users shall promptly remove any unauthorized personally-owned software from City IT resources upon receipt of a written request from the appropriate City personnel.
- 11.3 All software installed on City-owned IT resources that is not custom developed in-house by or on behalf of the City shall have a license certificate or documented proof of purchase of the license.

12. RESPONSIBILITIES

12.1 Records Retention Responsibilities for All users and City Departments

- 12.1.1 Use of City information and City IT resources may result in the creation of public records and data that the City may furnish to third parties in compliance with the TPIA or other legal obligation imposed on the City. (See, Records Retention Management Policy).

12.2 City Departments that have IT Infrastructure groups have the following responsibilities:

- 12.2.1 Developing and implementing procedures, auditing techniques, and assigning responsibilities to ensure that City employees, contractors, and other users of City IT resources adhere to this policy. Ensuring City employees are aware of and understand this policy and related procedures.
- 12.2.2 Distributing and communicating policies, standards, and guidelines to users.
- 12.2.3 Approving the use of City-owned and personally-owned mobile devices for City business by individuals under their supervision or areas of responsibility.
- 12.2.4 Installing, maintaining, and auditing the computing devices and networks owned, leased, or controlled by the City, but managed internally by the Department, to ensure only legal and acceptable use of such resources.

12.3 City Employees

- 12.3.1 With regards to all City information and City IT resources, regardless of the location of the City IT resource, City employees have the following responsibilities:
 - 12.3.1.1 Adhering to this policy and any additional City policies that augment this policy;
 - 12.3.1.2 Within 24 hours, reporting the loss of a City IT resource to the appropriate authorities and personnel in accordance with this policy;
 - 12.3.1.3 Within 24 hours, reporting to the appropriate authorities and personnel in accordance with this policy the loss of a personally-owned IT resource if the resource was used to conduct City business or otherwise risks the exposure of City information;

- 12.3.1.4 Providing information about the City IT resources to authorized personnel upon request;
- 12.3.1.5 Submitting City IT resources when requested to do so by authorized City personnel and prior to the employee's resignation, termination, or discharge from City employment;
- 12.3.1.6 Notifying designated City personnel as soon as possible prior to the City employee's departure and surrendering City IT resources to designated City personnel on or before the City employee's final day of employment, unless otherwise directed by authorized City personnel;
- 12.3.1.7 Responding to all requests issued by authorized personnel regarding City IT resources in a prompt, professional, and efficient manner; and
- 12.3.1.8 Upon completion of employment or a contract with the City:
 - (a) Transferring or causing to be transferred all City information to the City and City IT resources; and
 - (b) Backing up and removing from the City IT resource all personal records and information that is not City information or is not reasonably likely to qualify as City information.

12.4 In accordance with the requirements in this policy and other City policies, all users, including contractors and other non-City employees have the following responsibilities:

- 12.4.1 Complying with this policy and all other applicable City policies regarding City information and City IT resources;
- 12.4.2 Using and accessing City IT resources and City information in a lawful and ethical manner and only for their intended purpose in accordance with the authorization granted to the user by the City;
- 12.4.3 Operating IT resources in a safe manner in compliance with all applicable laws and City policies and in a manner that that is not reasonably likely to (a) create an unsafe work environment or (b) result in mistakes or actions that could present a real or imminent threat to the personal health and safety of the user, co-workers, and the general public. To the extent that this paragraph conflicts with any laws and City policies applicable to (a) emergency, public safety, or medical personnel, (b) the operation of an emergency vehicle, or (c) communicating with an emergency operator, public safety personnel, or medical provider regarding a medical or other emergency situation (e.g. a situation involving a reasonable belief that a person's life, health, or safety is in immediate danger), then those laws and City policies shall supersede this paragraph. This supremacy is limited solely to those specific points in conflict that relate to operating an IT resource in a safe manner;
- 12.4.4 Taking reasonable and necessary care to protect City IT resources and City information from unauthorized use or access, loss, damage, theft, abuse, or compromise;
- 12.4.5 Preserving and retaining configurations, security, and MDM software installed on City IT resources and any limitations imposed by the manufacturer;
- 12.4.6 Loading onto an IT resource only the minimum and essential City information necessary to perform the user's business function and accessing or storing this data for the minimum amount of time needed to perform the function;

- 12.4.7 Complying with instructions from authorized City personnel regarding the retention of records for purposes of complying with an open records request, discovery, legal matters, investigations and audits, or any other lawful purposes connected to or in furtherance of City business as directed by the authorized personnel. Upon receipt of an instruction to retain documents or ESI, the user shall not destroy or otherwise dispose of the ESI, regardless of the applicable retention policy, until the authorized City of Houston Legal personnel authorizes the disposition of the ESI;
- 12.4.8 Wherever possible, saving and storing City information on City IT resources, including transferring City information from mobile devices to the City's IT network, document retention repository, or archiving locations as soon as practicable;
- 12.4.9 Maintaining ESI according to City policies' and directives issued by appropriate City personnel or pursuant to the contractual relationship or agreement governing the contractor's performance and services;
- 12.4.10 Refraining from knowingly connecting any mobile devices to a computer or IT resource that does not have up-to-date and enabled anti-malware protection; and
- 12.4.11 Within 24 hours, reporting the following information to HITS, the applicable department, other appropriate authorities or City personnel:
 - 12.4.11.1 All lost or stolen mobile devices;
 - 12.4.11.2 Any known or suspected security violations or threats to City information and City IT resources;
 - 12.4.11.3 Any known or suspected incidents of unauthorized access or disclosure, or the inappropriate use of a City IT resource; and
 - 12.4.11.4 Any suspicions that malware has compromised a City IT resource.

13. EXCEPTIONS

- 13.1 Departments that are unable to follow any portion of this policy due to legacy technology use or other valid business reasons shall request an exception to the policy and seek approval through the process established in Administrative Procedure 8-3, Managing Exceptions Process.

14. COMPLIANCE

- 14.1 Users who violate or otherwise fail to adhere to this policy and all related City policies may be subject to appropriate disciplinary action, up to and including: immediate removal of any IT resources, whole or partially restricted access to City information and City IT resources, and termination or indefinite suspension.
- 14.2 Non-City employees, including contractors, who violate or otherwise fail to adhere to this policy and all related City policies may be subject to termination of contractual agreements or relationships, denial of access, and/or civil and criminal penalties.
- 14.3 Noncompliance with this policy and/or its resulting procedures may involve civil or criminal penalties, a requirement to pay fines, reimbursement expenses, and/or penalties assessed or imposed on the user.

14.4 The City may also pursue legal action for damages that arise as a result of the City employee's or contractor's breach or violation of this policy.

15. CONFLICT AND REPEAL

15.1 This Administrative Procedure supersedes Administrative Procedure 8-2, Procedure on Electronic Mail Communications, dated April 16, 2004, which shall be of no further force or effect.

15.2 If the provisions of this policy conflict with any law, that law shall prevail.