Administrative Policy

Acceptable Use of City Data, Information Systems

A.P. No.	A.P 8-1
Effective Date:	Upon Approval

1. POLICY STATEMENT

The City of Houston (City or COH) has adopted this Acceptable Use Policy (AUP) to protect City IT Resources against the backdrop of the City's culture of service, trust and integrity. COH is committed to educating employees and contractors about the importance of cyber security, and protecting COH data, systems and information from illegal or damaging actions by individuals. Maintaining effective security requires a team effort involving the participation and support of every user, so every user of City IT Resources is responsible for understanding and following this policy.

2. POLICY PURPOSE

This document establishes a City-wide policy for appropriate use, access, and maintenance of City information and City information technology (IT) resources, regardless of the physical location of the resource and information. Inappropriate use exposes the City and the user to unacceptable risks including malware attacks, ransomware, and data and information theft. This AUP sets out expected user behavior and delineates authorized and unauthorized operating practices to protect the City from those risks.

3. SCOPE

This policy applies to all City IT resources and IT resources accessing COH's non-public network. This policy applies to any person who is granted access, accesses, uses, or connects to City IT resources to conduct City business, including City employees, City officials, Mayoral appointees (boards, commissions, and authorities), vendors, contractors, independent contractors, consultants, interns, temporary employees, volunteers, users, or their guests. This policy does not apply to any device accessing the City's public network (e.g., publicly available Wi-Fi or computers at Houston Public libraries or community centers).

4. DEFINITIONS

City Employee: Any person who is employed by the City of Houston, all elected City officials, and all City temporary employees, interns and volunteers working at city facilities.

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 IT Asset: Any City-owned data, information, system, hardware, network, application, software, telephone or other device capable of storing, transmitting or receiving data owned, leased by, or operated by or on behalf 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. 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.

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 MS Teams chats, etc.) 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 and machine-readable materials.

Hacking/Hacking Tools: Behavior and tools designed to circumvent security measures, or to otherwise effect unauthorized changes or access to computer hardware, software, systems, networks, or data.

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

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 IT Device: Any device owned, paid for (whether in whole or in part), leased, or issued by any person or entity other than the City that can be carried by a person or is generally intended to be portable and the device transmits voice or data wirelessly, or through a cellular network, Wi-Fi, or Internet connection, even temporarily. Personal IT devices also include machine to machine (M2M) devices that utilize cellular or wireless communications, even if the devices are not portable. Examples of personal IT devices that transmit voice or data using wireless, Wi-Fi, or cellular services include notepads, laptops, tablet PCs, tablets, smartphones, and cell phones.

Privileged User Accounts: Accounts with an elevated level of permissions designed to allow for the installation or configuration of software on any City IT Asset. Additionally, privileged user accounts also allow for elevated access to City Information.

Sensitive Information: Information deemed by the City or by law to be sensitive in nature such that it 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 also has the meaning ascribed to “personal identifying information” and “sensitive personal information” in Tex. Bus. & Com. Code § 521.002, as may be amended from time to time. Sensitive information may include credit card numbers, social security numbers, driver’s license numbers, date and place of birth, financial information, criminal history, protected health information, and information protected by non-disclosure obligations.

Social Media: Refers to internet-based technology communications tools with a focus on immediacy, interactivity, user participation, and information sharing. These venues include social networking sites, forums, weblogs (blogs, vlogs, microblogs), online chat sites, and video/photo posting sites or any other such similar output or format. Examples include Facebook, Twitter, and YouTube.

User: Any person who is granted access, accesses, uses, or connects to City IT Resources to conduct City business, including but not limited to City employees, City officials, Mayoral appointees (boards, commissions, and authorities), vendors, contractors, independent contractors, consultants, interns, temporary employees, volunteers, or their guests.

Unsolicited e-mail: Any e-mail message received from an unknown, suspicious, or untrustworthy source or via a mass mailing list to which the recipient did not subscribe.

Voice over Internet Protocol (VoIP): A method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks (e.g., Internet).

5. GENERAL EXPECTATIONS

5.1. Users are responsible for maintaining the security of their COH accounts (e.g., e-mail, domain, applications, databases, etc.) and taking precautions to prevent unauthorized access, including but not limited to safeguarding access to their passwords, codes, and credentials.

5.2. Users must take reasonable precautions to protect City IT Resources, data and information from loss or damage.

5.3. Users are prohibited from intentionally or 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 or knowingly avoiding, disabling, or circumventing City-established security procedures and controls, or sharing or disclosing user account passwords.

5.4. Users shall not leave the workstation without first turning off or locking the workstation, such as by utilizing Control+Alt+Delete to lock workstations.

5.5. Users must not share user account passwords under any circumstance.

5.6. Users must not bring personal equipment such as wireless keyboards and mice, personally-owned monitors, or storage devices, to City facilities and install it on City equipment. While working remotely at a telework site as defined in A.P. 3-36, Hybrid-Telework Program, Users may connect personal equipment, such as personal mice, printers, or monitors, to City laptops.

5.7. Users are not allowed to install unauthorized software on City IT Resources. To be authorized, software must be on the City of Houston IT Services (HITS) approved list of allowed software/application or otherwise be approved in writing by the City's Chief Information Officer (CIO) or Chief Information Security Officer (CISO) prior to its installation. HITS will maintain an approved list of software that employees can access.

5.8. Users must not clear the application, security, system or browser event logs and history logs.

5.9. Users must not open any files or macros attached to an unsolicited e-mail. These messages can include pornographic topics, hoax messages, chain e-mail, spam messages and advertisement messages. Users may report suspicious e-mails by clicking the "Report Phishing" button in the Outlook ribbon or sending to Security.OperationsCenter@houstontx.gov.

5.10. Users must not create, copy, transmit, or retransmit chain letters or other non-City-sanctioned mass mailings regardless of the subject matter.

5.11. Users must delete spam and other junk e-mail without forwarding it unless the user is reporting the email to the COH Cyber Division as stated in paragraph 5.9.

5.12. Users must not click on or follow any hyperlinks or URLs included in an unsolicited e-mail message.

5.13. When conducting City business via email, employees and contractors issued City email accounts must use their official City email address and account to transmit or store City Information or otherwise conduct City business. Use of third-party email services, such as Gmail, to conduct City business is prohibited

5.14. Users must not automatically forward e-mail messages to non-COH accounts (e.g., Yahoo, Gmail, Hotmail, Comcast, etc.).

5.15. COH users must encrypt known Sensitive Information sent via e-mail if the recipient is external to COH.

5.16. Users with privileged user accounts must not use their privileged accounts to access COH email. All users must use their normal user (non-privileged) account to access their own COH email mailbox to send and receive email. Users assigned privileged user accounts must not use their privileged accounts for Internet browsing or other Internet connections. Users assigned privileged accounts with privileged access must use those accounts only when required to perform system administrative duties and responsibilities.

6. PRIVACY EXPECTATIONS

6.1. In accordance with and subject to COH policies and applicable laws, COH has the right to and may, at any time, research, monitor, collect, log, audit, inspect, intercept, record, read, search, seize or copy all data and information residing on COH systems without notice to users.

6.2. Users do not have a right to privacy or a reasonable expectation of privacy while using any City IT resources at any time, including but not limited to when using City IT resources to access the Internet, or e-mail, as well as other communications such as texts, cell phone records and instant messages. By using City IT resources, users give their consent to the City to monitor and view the contents of any files or information maintained using this equipment. In addition to being monitored by COH Cyber Division personnel, data and information maintained on City IT resources may be subject to disclosure under the Texas Public Information Act (TPIA) and through legal process.

6.3. COH reserves the right to monitor and audit networks and systems periodically to ensure the security of the network and compliance with this policy.

6.4. Auditing and inspecting City IT Assets for the presence of illegal or unlicensed software may be conducted at any time.

6.5. Absent authorized investigative purposes, users are prohibited from collecting and monitoring location or GPS tracking information that may be obtained as part of the normal management and administration of City IT Assets.

7. SYSTEM, DATA AND INFORMATION OWNERSHIP

7.1. All City Information and City IT resources are the property of the COH, including but not limited to all City information created or generated by, accessed from, backed up, or stored on COH-owned mobile devices or transferred to personal IT resources. Beginning on June 30, 2024, any Personal IT device used to conduct City business requires prior approval from the CIO or CISO, and the installation of the City administered Mobile Device Management (MDM) solution. In consultation with the City Attorney, the CIO and CISO shall be responsible for establishing employe notifications and required forms for the implementation and administration of the MDM solution on Personal IT devices. Personal IT devices used to conduct City business may be subject to inspection by law enforcement authorities or appropriate City personnel, including but not limited to the City's CIO, CISO, Office of Inspector General during or pursuant to an investigation or by the City Attorney's Office pursuant to a TPIA request or a discovery or subpoena request during litigation.

7.2. Users are responsible for properly caring for, securing and maintaining City IT Assets issued to them and must use reasonable efforts to protect them from theft, damage, abuse and unauthorized use. Users should not leave City's IT assets like laptops, tablets, city mobile devices or other similar devices in vehicles. Users experiencing the loss or theft of a City IT Asset may be subject to corrective action up to and including payment for device replacement, and indefinite suspension or and termination. Except as provided in Section 9, Replacement of Mobile Devices, in A.P. 8-8, Mobile Device Eligibility, if the City IT Asset issued to the User is lost, broken, or stolen, the user may be requested to reimburse the City for the cost of City IT asset.

7.3. If a City IT asset containing City Information or data or Personal IT device upon which the City MDM solution is installed is lost or stolen, the user must promptly, but at least within 24 hours of discovering the incident, notify the user's manager and send an email to Security.OperationsCenter@houstontx.gov so the appropriate steps can be taken to protect City Information. In the case of a stolen city mobile device, laptop, tablet, or similar City IT asset containing City Information, the user must also file a police report and provide a copy of the report to the CISO.

8. LIMITED PERSONAL USE

8.1. Users may use City IT Resources only for secure, incidental personal use.

8.2. Users should use good judgment when using City IT resources for limited personal use, which includes but is not limited to ensuring the use has no or minimal cost to the City, does not negatively impact overall employee productivity, results in minimal wear and tear to the device, and the use would not negatively reflect on the City.

9. UNAUTHORIZED USES AND SPECIFIC PROHIBITIONS

9.1. The following list of activities and uses of City information and City IT resources are strictly prohibited at any time by any user, unless performed (a) for investigative purposes; (b) by the COH Cyber Division or Office of Inspector General (OIG), in the course of legitimate job responsibilities; or (c) for other lawful purposes as expressly authorized in writing by the CIO or CISO.

9.2. The below list is not exhaustive, but instead provides guidance regarding the types of activities that constitute Prohibited Uses.

9.2.1. Creating, copying, transmitting, or retransmitting large file attachments that can degrade the performance of the entire COH network, such as greeting cards, videos, or sound files.

9.2.2. Accessing or attempting to access, create, download, view, store and/or transmit adult content, including but not limited to pornography or sexually explicit materials.

9.2.3. Accessing online gambling (legal and illegal) and/or online gaming sites.

9.2.4. Accessing online dating services.

9.2.5. Accessing sites that promote illegal activity or copyright violations.

9.2.6. Accessing third-party email (e.g., Gmail, Yahoo, Hotmail, etc.) or storage (e.g., Dropbox, Box, Google Drive, etc.) services from COH IT resources.

9.2.7. Intentionally using the User's personal email address or email account to send or transmit City Information, where the User has a City email account.

9.2.8. Intentionally storing City Information in third-party storage accounts or using third-party storage services (e.g., Dropbox, Box, Google Drive, etc.).

9.2.9. Accessing or using City IT resources to engage in any activity that is illegal under local, state, or federal law, as well as any activity that is otherwise prohibited by City policies and executive orders. Such activities include but are not limited to hate speech or material that ridicules others based on race, color, national origin, gender, sexual orientation, gender identity, religion, or disability.

9.2.10. Using City IT Resources as a staging ground or platform to gain unauthorized access to other systems.

9.2.11. Hacking or using hacking tools or malware to circumvent security measures.

9.3. City employees using City IT resources for commercial purposes, private gain, in support of "for profit" activities, in support of outside employment of self or others, or for conducting business activity (including but not limited to paid consulting, sales, or administration of business transactions.)

9.4. Intentionally or knowingly causing security breaches or engaging in activities that could reasonably be expected to compromise the security of or harm any City IT Resources, such as avoiding, disabling, or circumventing COH-established cyber security procedures and controls; sharing or disclosing a person's user ID or other means of digital authentication (including passwords); jail-breaking a COH mobile device or using a jailbroken device to conduct COH business, or introducing, uploading, downloading, or distributing malware.

9.5. Downloading, copying, and/or playing computer video games.

9.6. 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.

9.7. Posting non-public City information to external newsgroups, bulletin boards, social media (including but not limited to Facebook, Twitter, etc.), or other public forums without authority, including but not limited to postings that could reasonably be expected to create the perception that the communication was made in an official City capacity.

9.8. Violating intellectual property rights (i.e., patent, copyrights or trademarks), including but not limited to acquiring, using, reproducing, transmitting, or distributing software or data or materials not licensed for use by the User or the City.

9.9. Exporting, re-export, transferring, or disclosing export-controlled software or data in violation of applicable licensing restrictions, laws and regulations.

9.10. Downloading or installing software, freeware/shareware or executable program files from the Internet or other electronic sources onto City IT resources without advance approval from the COH Cyber Division, including but not limited to games, scanners, password-crackers, anti-malware software, client firewalls, web browsers, etc.

9.11. Downloading files, for example, music, to forward to another individual ("file sharing"), which is outside the scope of limited personal use and is not in connection with conducting City business.

9.12. Using or installing unauthorized instant messaging applications or platforms.

9.13. Using unauthorized Peer-2-Peer Networking software.

9.14. Intentionally storing COH files and data on personal IT devices without the implementation of the City administered mobile device management solution on or after June 30, 2024.

9.15. Using City information and City IT resources for any other purpose outside of the acceptable uses authorized by this policy or other COH policies.

10. INTERNATIONAL TRAVEL

10.1. All City employees traveling outside the United States may not access City information and City IT resources on mobile devices (e.g., City issued and personal smart phones, personal smart phones, laptops, tablets, etc.) while connected to any public Internet service (e.g., hotel, restaurant, coffee shop, etc.). Instead, City employees required to work on City business while abroad or who anticipate accessing City IT resources or City Information while abroad, must obtain City-provided Internet hotspots prior to departure. At least 14 calendar days prior to travelling internationally on city business or when on personal leave and the city employee anticipates the need to access City IT resources or City Information while outside the country, the City employee must send notification to Security.OperationsCenter@houstontx.gov for further instructions.

10.2. Failure to send the notification or otherwise comply with section 10.1 of this policy may result in temporary account deactivation.

11. COMPLIANCE

11.1. Users who violate or otherwise fail to adhere to this policy may be subject to appropriate corrective action, up to and including indefinite suspension or termination. In addition, the City employee who violates or otherwise fails to adhere to this policy may be subject to immediate removal of any City IT resources, or whole or partially restricted access to City IT resources.

11.2. Non-City employees, including contractors, who violate or otherwise fail to adhere to this policy and may be subject to termination of City contracts or business relationships, or denial of access.

11.3. Noncompliance with this policy may result in civil or criminal penalties, reimbursement requirements, and/or contractual breaches. COH may also pursue legal action against violators for damages that arise from violations of this policy.

12. EXCEPTIONS

12.1. Users that are unable to follow any portion of this policy shall request an exception to the policy from the CIO or CISO, as applicable, or shall seek approval through the process established in A.P. 8-3: Managing IT Policy Exceptions Policy.

13. CONFLICT AND REPEAL

13.1. This Administrative Procedure supersedes Administrative Procedure 8-1, Use of City Information and City Information Technology Resource, dated October 17, 2014, which shall be of no further force or effect.

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

14. RELATED DOCUMENTS AND INFORMATION

- A.P. 8-3: Managing IT Policy Exceptions Policy

15. POLICY SPONSOR

Department: Houston information Technology Services (HITS)