CITY OF SAN ANTONIO

Administrative Directive	**7.4A Acceptable Use of Information Technology**
Procedural Guidelines	Regarding use of electronic communications systems
Department/Division	Information Technology Services Department (ITSD)
Effective Date	April 1, 2014
Revisions Date(s)	December 14, 2017
Review Date	
Owner	Patsy Boozer, CISO

Purpose

This Administrative Directive (AD) provides guidance for the acceptable use of information technology systems including electronic devices, electronic mail, Internet access, and/or software among other City systems. This includes acceptable use of City-owned computers, mobile devices and/or personal. This directive establishes and identifies responsibility for the acceptable use of technology to help ensure the confidentiality, integrity and availability of City systems.

The City of San Antonio (COSA or City) provides access and use of its information technology systems to help users efficiently and effectively perform their business-related activities. All users of the City's information technology systems are responsible for using that technology in an appropriate and lawful manner.

Inappropriate use of information technology exposes the City to additional internal and/or external vulnerabilities that may reduce the reliability, confidentiality, integrity and/or availability of those systems.

The Information Technology Services Department (ITSD) shall be responsible for developing, maintaining, publishing and administering the acceptable use of information technology assets and systems. All unauthorized access to City data is strictly prohibited.

The City's information technology systems are shared resources that serve all of its users and provide the general public with access to its website. Inappropriate use of information system assets reduces the usefulness of these resources.

Policy Applies To

☒ External & Internal Applicants	☒ Temporary Employees
☒ Full-Time Employees	☒ Volunteers
☒ Part-Time Employees	☒ Grant-Funded Employees
☒ Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	☒ Vendors, Contractors and Other Third Parties

Definitions	
Bring Your Own Device (BYOD)	The practice of allowing the employees of an organization to use their own computers, smartphones, or other devices for work purposes.
City-administered information technology systems	Any technology or equipment that is used and/or managed by the City even if the City does not own the technology or equipment. City-managed information technology systems include technology or equipment owned by the City, on loan to the City, funded by grants, leased by the City, etc. Information Technology systems includes but, are not limited to computers, mobile communication devices, telecommunication devices, servers, networks, software, databases and email messages, among other physical and virtual infrastructure.
Digital Signature	An electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature.
Electronic mail	An electronic government record sent and received in the form of a message on an electronic mail system of a government, including any attachments, transmitted with record the message.
Electronic Record	Record created, generated, sent, communicated, received, or stored by electronic means.
Electronic Signature	An electronic sound, symbol, or process attached to, or logically associated with a record and executed or adopted by a person with the intent to sign the record.
Generic Account	A generic account is any non-person account that may allow multiple users to use a single account to authenticate to the City network, application or other resource.
Incidental Use	Personal use of technology that does not interfere with the performance of assigned duties, does not have a detrimental effect on City information technology systems, and is not prohibited by this policy.
Local Government Record Retention Schedules	Publications issued by the Texas State Library and Archives Commission under the authority of Subchapter J, Chapter 441 of the Government Code which establish the mandatory minimum retention period for a local government record
Malware	Malicious software designed to impact the confidentiality, integrity and/or availability of an information technology system. Malware can include viruses, worm, Trojan Horse, or adware among other malicious programs.
Network	A group of two or more computers linked together to facilitate communication, data sharing and processing among other computer activities.
Records Management Officer	The person who administers the records management program established in each local government under section 203.026, chapter 203 of Local Government Code.
Retention Period	The minimum time that must pass after the creation, recording or receipt of a record or the fulfillment of certain actions associated with a record before it is eligible for destruction.

Software	**Authorized Software-** Authorized software is any program, code or installable executable file that has been tested and approved by ITSD. Authorized software constitutes any program, code or executable file deemed necessary to meet business needs. This includes Shareware, Freeware and Open Source software that meets the criteria stated in this policy. **Unauthorized Software-** Unauthorized software is any program, code or installable executable file that has not be tested and approved by ITSD or not necessary for business needs. This includes Shareware, Freeware, Open Source pirated software or copyright infringement in the use of software. For purposes of this policy, pirated software or copyright infringement includes illegally copied and/or downloaded software that violates licensing restrictions.
Sponsor	Departmental representative responsible for authorizing non-employee access to COSA assets and/or systems.
User	Any employee or non-employee who uses COSA-administered information assets and/or systems, exclusive of COSA's web pages

Policy

COSA is required to protect public assets and resources, and it has an obligation to manage information technology systems to comply with Chapter 552 of the Texas Public Information Act (open public records), Sections 7.71-7.79 of the Texas Administrative Code and 205.001-205.009 of the Local Government Code, among other regulations.

The National Institute of Standards of Technology (NIST) and industry best practices has been adopted by the City to help maintain the confidentiality, integrity and availability of COSA systems.

This directive pertains to all information collected or maintained by or on behalf of the City and all information assets used or operated by the City, a City contractor, a City vendor, or any other organization on behalf of the City.

- All information technology assets and systems, procured with City funds and/or used in the conduct of City business.
- All access to the City's facilities and networks, data, and/or applications among other systems including employees, contractors, vendors, and other third parties of City information assets, systems.
- All electronic messaging, equipment, or technology that is owned or administered by the City including City-owned computers, mobile devices, and/or personal devices is included within the scope of this Directive.
- All software, information systems and/or other documents developed by City personnel with City funds or licensed to the City of San Antonio.
- All data processed, stored, and/or transmitted by any City information technology system.
- All devices that use the COSA network, including any "Bring Your Own Device" (BYOD).

Adherence to this directive will help assure the City's acceptable use of technology.

- City-managed information technology systems shall be used for official business only, which may include personal communications, including telephone calls during business hours, that are necessary and in the interest of the City. While some incidental use (as defined below) of City-managed technology is unavoidable, such incidental use is not a right, and should never interfere with the performance of duties or service to the public.
- There shall be no expectation of privacy when using any City-administered information

technology system including internet access for any information input or reviewed from City or personal accounts while in contact with City systems, social media, personal email accounts, SMS messages or instant messaging.

- All information generated, processed, stored, or entrusted on any City-provided information technology system is the property of COSA.
- COSA data shall be stored on network drives and not local drives. Local drives are not included in the City's backup strategy.
- Protected data per AD 7.3A Data Security (e.g. HIPAA, CJIS, Sensitive Personally Identifiable Information (PII) stored on laptop hard drives or removable media shall be authorized by the data owner and use ITSD approved encryption.
- Externally transmitted data by any technological means that contains protected data per AD 7.3A Data Security (e.g. HIPAA, CJIS, and Sensitive PII) shall use ITSD approved encryption.
- Business email received on COSA account shall not be manually or automatically forwarded or redirected to email addresses outside of COSA.
- A generic login account will only be allowed for specific business need. A written justification must be submitted to ITSD for approval. Generic network user account will not have email access.
- Email messages not essential to the fulfillment of statutory obligations or to the documentation of the City's functions may be deleted. Note: These messages may include personal messages, internal meeting notices, letters of transmittal, and general FYI announcements.
- Email messages that fulfill statutory obligations or document the City's functions are subject to retention as established by the Texas Administrative Code referenced in the Retention and Disposition of Email section.
- Individual COSA email accounts may not be used to send to more than 50 recipients of the same email message.
- Emails in deleted folder will be purged after 14 days.
- City distribution list shall not be made available for use by external email accounts.
- Distribution list must be maintained by owner to remove invalid email addresses.

Personal Use Policy

Personal use of technology must not interfere with the performance of assigned duties, must not have a detrimental effect on any City information technology system, and not be prohibited by this policy.

This includes the personal use of City-owned or managed technology that:

- Does not cause any additional expense to the City and is infrequent and brief
- Does not have a negative impact on overall user productivity
- Does not interfere with the normal operations of the user's department or work unit and does not compromise the City in anyway
- Does not embarrass either the City or the user
- Does not contravene other elements of this policy and serves the interest of the City in allowing employees to address personal matters which cannot be addressed outside of work hours without leaving the workplace.

Examples of personal communications that can be in the interest of the City include:

- Communications to alert household members about working late or other schedule changes
- Communications to make alternative child care arrangements, communications with doctors, hospital staff or day care providers
- Communications to determine the safety of family or household members, particularly in an emergency communications to reach businesses or governmental agencies that only can be

contacted during work hours and communications to arrange emergency repairs to vehicles or residences.

Security and Proprietary Information

Information stored on any City-administered information technology system should be classified in accordance with federal, state and local statues, ordinances, regulations, and/or policies among other directives regarding the confidentiality of the information (AD 7.3a Data Security). Users must comply with all City Directives regarding use of information technology, including:

- Electronic Communications (e-mail, voice and Internet)
- Password Management
- Security
- Data Management and Classification Monitoring
- Remote Access

All personal computers, laptops, and workstations should be protected from unauthorized access when the system is unattended. The recommended method of security for City devices is with a password-protected screensaver (with the automatic activation feature set to 15 minutes or less) or by manually locking the device (Ctrl-Alt-Delete for most Microsoft Operating Systems). Devices that cannot be locked as described above should be secured by logging off the devices or turning them off.

1. All BYOD devices used for work related tasks must be in compliance with AD 7.10 Mobile Device Security in order to obtain COSA email access; remote access etc. and the owner of the device must install and maintain security related software (operating system updates, Anti-virus/malware protection, etc.). ITSD has the right to refuse the use of any personal device for COSA related use if the device cannot be secured based on the standards and policies stated in this document. It is the responsibility of the owner to report if the device is lost or stolen immediately to ITSD.
2. User must take reasonable and necessary precautions to secure and protect electronic devices.
3. ITSD regularly maintains operating systems, updates security software, and applies security patches by sending those updates during non-business hours to computers attached to the network. When a user leaves for the day, he/she must log off from his/her computer, but leave the computer turned on and attached to the network. Laptops must be connected to the network at least once a month for at least 24 hours in order to receive updates.
4. As a regular maintenance step, at least once a week, save and close open files and applications then power off computer completely. Once the computer has powered down, power it back on. As computers are used on a daily basis, applications, files opened and web browsing slowly consume available memory and resources which over time cause computer to slow down. Refreshing the computer's resources at least once a week, will keep it running at an optimal speed with fewer problems in the long term.
5. All technology devices used by a technology user to connect to the City's networks shall continually execute approved security software with a current virus definition file. This includes user-owned equipment attached to the City's networks through remote access technologies. The City is not responsible for providing the required security software for user-owned computers.
6. E-mail attachments that may constitute a risk to the City's technology environment will be removed from e-mail messages passing through the City's mail servers. Removed attachments are replaced by a message indicating that they have been removed and the header and text of the original message delivered normally.
7. A spam message filter is used to reduce the transmission of chain letters, broadcast announcements, general advertisement postings, or any other message via e-mail to a group of persons not requesting the message.
8. Sensitive information should not be stored on removable media unless it is required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in

accordance with ITSD Security policies regarding encryption.

9. Only software that has been approved by ITSD may be installed on City owned devices. If an employee needs to have software installed on a City owned device they must submit a request to ITSD stating the business need for the software as well as any other information relevant to justify the use of the requested software. No City employee or approved contractor or vendor will install, reproduce, distribute, transmit, download, or otherwise use any software unless such software has been approved by ITSD and properly licensed. ITSD will monitor for unapproved/unauthorized software and reserves the right to remove any software from City owned devices ITSD will maintain an approved list of software that employees can access.

Password Management

Passwords are an important element of the acceptable use of technology and associated information security. A poorly chosen password may result in the compromise of the City's network. All technology users are responsible for taking appropriate steps to select and secure passwords. Users shall take reasonable and necessary care to prevent unauthorized access to workstations, laptops, applications, mobile and/or other devices.

City Password requirements (at a minimum):

1. No departmental personnel, including administrative staff, shall request access to or maintain lists of other user passwords.
2. User account must use a "strong" password.

   Strong passwords are defined as:
   - At least eight characters in length
   - Not based on words in any language, slang, dialect or jargon
   - Not based on personal information, such as family names
   - Not common usage words like family, pets, friends, COSA, birthdays, phone numbers, addresses, computer terms, fantasy characters and/or common patterns like aaabbb, qwerty, zyxwvuts, 123321 or any derivation followed by a digit.
   - Contain at least one (1) each of the following
     - English uppercase (A through Z),
     - Lowercase (a through z),
     - digit (0 to 9) and
     - non-alphanumeric character (!,$,#,%)
3. All users' passwords will expire at intervals of ninety (90) days. Users will be prompted to change passwords beginning 10 days before the next expiration date. Passwords may not be re-used.
4. Passwords will be changed immediately after a security breach has been detected to the affected COSA systems.
5. As the COSA system software permits, an initial or reset password issued to a user will be valid only for the user's next log in. After that, the user must be prompted to change their password.
6. Users must enroll in the COSA Self-Service Password management system which provides expiration notifications and allows network passwords to be reset from desktop, laptop or mobile device.
7. Password Protection Guidelines:
   - Do not write passwords down, store them on-line, or reveal them in any electronic format.
   - Do not use the same password for COSA accounts as for other accounts (i.e. social media, personal email account, banking sites, etc.).
   - Passwords must be treated as sensitive and confidential information thus do not share City passwords with anyone.
   - ITSD support personnel may require a user to enter their password in order to resolve a problem.

- Do not talk about a password in the presence of others.
- Do not hint at the format of a password ("my family name").
- Do not click on links in emails from unknown sources; look for the "External" tag to identify email from outside of COSA.
- Do not provide account information that includes personal information and/or password.
- Do not reveal a password on questionnaires or security forms.
- Do not use the "remember password" feature.
- Do not store passwords in a file on ANY computer system without encryption.

8. COSA passwords are not to be reused or similar to any non-work related passwords for accounts such as personal email accounts or social media accounts
9. Technology users shall report any suspected security violations or threat to the ITSD Service Desk immediately. Any activity performed under a user-id/password combination is presumed to have been performed by that user and is the responsibility of that technology user.

Retention and Disposition of Email

The City's approved Declaration of Compliance with the Local Government Records Retention Schedules establishes record series and the retention period for each series All Email sent or received by a government is considered a government record. Therefore, all electronic messages must be retained and disposed of according to the City's retention requirements as described in Records Management: A.D 1.34: Records Management for Physical Electronic Records. Full detail of A.D. 1.34 can be sourced from Office of the City Clerk or **http://www.sanantonio.gov/hr/admin_directives/index.asp** . Users and their supervisors or sponsor should seek guidance from the City's Records Management Officer if there is a question concerning whether an electronic message should be deleted.

1. Electronic Mail (E-mail), Instant Messaging, Voicemail, and Text Messaging:

a. All electronic mail messages, instant messages, voicemail and text messages regarding City business must be retained and disposed of according to the City's retention requirements. It is the content and function of the record that determines the retention period for that message (A.D.1.34).

b. The City's electronic mail system is not a records management system. Electronic messages that the user determines, based on the Local Government Records Retention Schedules, are subject to retention for more than 30 days should be moved from the user's "Inbox" and/or "Sent Items" folders within 30 days of its receipt or creation. Emails in deleted folder will be purged after 14 days and electronic messages will be automatically deleted after 1 year. Electronic messages to be retained longer than 1 year may be placed in folders and saved on a network drive, or transferred to an automated records management software application.

Acceptable Use of Electronic Signatures and Electronic Records

Electronic signatures, an automated function that replaces a handwritten signature with a system generated signature statement, and electronic records can be utilized as a means for authentication of City documents, computer generated City documents and/or electronic City entries among other uses. System generated electronic signatures are considered legally binding as a means to identify the author of record for entries and confirm that the contents of what the author intended. City departments and staff will be allowed to utilize electronic signature in accordance with this directive, City, State, and/or Federal regulations regarding such.

Acceptable Use of Electronic Records and Electronic Signatures are allowed:

1. Where policies, laws, regulations, and rules require a signature and that requirement is met if the document contains an electronic signature.

2. Where policies, laws, regulations, and/or rules require a written document and that requirement is met if the document is an electronic record.
3. Where each party to a transaction must agree to conduct the transaction electronically in order for the electronic transaction to be valid and binding. Consent may be implied from the circumstances, except with respect to any electronic records used to deliver information for which consumers are otherwise entitled by law to receive in paper or hardcopy form.
4. If a law prohibits a transaction from occurring electronically, the transaction must occur in the manner specified by law.
5. If a law requires an electronic signature to contain specific elements, the electronic signature must contain the elements specified by law.
6. If a law requires that a record be retained, that requirement is satisfied by retaining an electronic record of the information in a record that accurately reflects the information set forth in the original record and shall remain accessible for later reference. When the requirements for retention require an original form, retention by an "electronic form" shall provide and satisfy the retention requirement.

Procedures, Forms, Guidelines and Resources for electronic signatures:

1. Procedures for electronic signatures can be found under the Texas Uniform Electronic Transactions Act
2. United States governance can be found in 18 USC 2510, Electronic Communications Privacy Act
3. Record management for COSA is established by Local Government Code: 201 through 205. The Texas State legislature requires local governments to establish a records program by Ordinance.
4. City of San Antonio adopted Ordinance 70508 and 72054
5. Ordinance 70508 (11-02-1989) names the City Clerk as the City's Record Management Officer
6. Ordinance 72054 (August 9, 1990) establishes the City's Records Management program
7. The charter of the City of San Antonio mandates that the City Clerk shall keep the records of the Council and of the City
8. Pursuant to Article II, Section 10 of the City Charter, the City Clerk shall keep the records of the Council and of the City. Pursuant to City Ordinance 72054 which establishes the City's records management program in compliance with the Local Government Records Act and reaffirms City Ordinance 70508 naming the City Clerk as the City's Records Management Officer, both ordinances filed with the Texas State Library and Archives Commission, the Records Management Officer shall develop policies and procedures in the administration of the City's records management program.
9. This policy does not supersede any local, state or federal laws regarding records management, confidentiality, information dissemination or standards of conduct.

Electronic Transactions and Signed Records:

1. Electronic Records - The Uniform Electronic Transactions Act (UETA) was enacted into law in Texas by the 77th Legislature (Senate Bill 393) in May 2001, and became effective on January 1, 2002. UETA provides definitions for several key terms that pertain to this policy. These terms are listed in the "Definition" section of this directive.
2. Electronic Signatures - Texas law (Government Code, Section 2054.60, provides a definition for the term "digital signature," which is sometimes used interchangeably with "electronic signature" (see Section II, C, 3).

Unacceptable Use of COSA Resources and the Internet

The following activities are prohibited unless performed in the course of legitimate job responsibilities. The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable uses of COSA information technology systems:

1. The registration or use of any COSA related email addresses for personal accounts such as personal Email, Social Network accounts (Facebook, Twitter, LinkedIn, etc.), personal billing services (utilities, cell phone, cable, insurance, cloud based services, etc.) or any other non-work related sites.
2. Engaging in any activity that is illegal under local, state and/or federal statutes as well as any activity that violates COSA policies and Administrative Directives.
3. Accessing, displaying, storing or transmitting material that is offensive in nature, including sexually explicit materials, or any text or image that can be considered threatening, racially offensive, or hate speech. This includes any images, text, files, etc. sent electronically to co-workers or outside parties. Accessing, storing, displaying, or transmitting pornographic materials using City-owned and managed technology is strictly forbidden.
4. Engaging in any form of harassment, whether sexual or otherwise, or sending any unwelcome personal communication. It is the perception of the recipient that prevails in most instances, not the intent of the sender. Harassment may be construed as any written, verbal or physical conduct designed to threaten, intimidate, coerce, taunt or bully the recipient or another individual.
5. Any personal use that interrupts City business and that keeps an employee from performing his/her work.
6. City systems shall not be used to chat online, "blog", or shop online if not authorized by Department Director as part of the users job function.
7. Extensive personal use of the Internet for any non-work-related purpose during working hours which decreases the employees productivity or results in decreased performance of the City's Internet facilities.
8. Violating any copyright, trade secret, patent and/or other intellectual property or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City.
9. Unauthorized downloading of and/or distributing of copyrighted materials.
10. Revealing a City account password to others or allowing use of a City account by others. This includes household members, coworkers, vendors, contractors and visitors when work is being done at home. Revealing a City account password to an authorized technician during a troubleshooting procedure is not a violation of this policy. In such a situation, a new password should be established as soon as possible, after the problem is resolved.
11. Requesting a password to another users network or application account.
12. Unauthorized reading, deleting, copying, modifying, printing and/or forwarding of electronic communications of another, or accessing electronic files of another without authorization.
13. Unauthorized duplication of copyrighted material including, but not limited to, text and photographs from magazines, books or other copyrighted sources, copyrighted music and/or copyrighted movies. Copying or installing copyrighted software for which the City or the end user does not have an active license is not permitted.
14. Sending SPAM to either internal or external parties. Individual email accounts will be limited by technical controls as a preventive measure to detect SPAM originating from a City email account. Large volume emails to recipients will not be allowed from individual email accounts. Request for approved email accounts designated for such business purposes will be submitted to ITSD Customer Service.
15. Approved email accounts must not regularly send bulk emails unless distribution lists are maintained. All undeliverable or invalid addresses from distribution lists must be regularly removed to prevent the City from not being able to send email through Internet Service Providers and/or mail hosts.

16. Downloading and/or copying music, photographs or video material, including such material that has been obtained legally, onto City computers or servers.
17. Downloading and/or installing executable program files from external media or the Internet without the approval of ITSD.
18. Exporting software, technical information, encryption software and/or technology, in violation of international or regional export control laws.
19. Using the City's electronic mail or Internet systems for private gain or profit.
20. Using unauthorized personal software which allows peer-to-peer communications between two workstations (Yahoo Messenger, Skype, Snapchat, Periscope, Instagram, Facebook Messenger, etc.).
21. Using instant messaging through public service providers.
22. Using City systems for non-work-related access to online auctions or ecommerce sites (such as e-Bay, Amazon).
23. Maliciously introducing malware or similar programs into the network or server.
24. Soliciting for political, religious, and/or other non-business uses not authorized by COSA.
25. Making fraudulent offers of products or services originating from any City account.
26. Accessing non-business related streaming media, including Internet-based radio.
27. Accessing any non-business related application which maintains a persistent application connection to the Internet, such as streaming videos or media, such as Pandora, Netflix, and/or Google Video, among others.
28. Using City technology, electronic mail and/or Internet facilities for political activity including voting, private gain, gambling, shipping, games, entertainment or other non-business function unless permitted by this directive.
29. Including email "tag lines" or personal quotations other than ones that state the mission of the City or the user's Department.
30. Using the COSA email system to automatically forward COSA email to a non-city email account is prohibited.
31. Sending or forwarding junk e-mail, chain letters, or other mass mailings.
32. Causing security breaches or disruptions of City communications. Security breaches or disruptions can include, but are not limited to:

    - Accessing data which the user is not authorized to access or logging into a server or user account that the user is not expressly authorized to access
    - Causing network disruptions for malicious purposes including, but not limited to, network sniffing, ping floods, packet spoofing, denial of service of any kind, and forged routing information for malicious purposes
    - Port scanning or vulnerability scanning for malicious purposes is prohibited. Non-malicious scanning that is part of a City-sanctioned security process is allowed. ITSD should be notified prior to any such scanning
    - Circumventing user authentication or security of any device, network or account
    - Maliciously interfering with or denying service through a denial of service attack, or by other means
    - Using any program/script/command, or sending messages of any kind, with the intent to interfere with, and/or disable, another user’s device or session, via any means, locally or via the City’s network
    - Adding/removing hardware components, attaching external devices, and/or making configuration changes to information technology devices without the explicit approval by ITSD
    - Storing confidential data on personally owned devices.

Privacy and Monitoring

1. City systems may be monitored by ITSD to support operational, maintenance, auditing, security and/or investigative activities including enforcement of this Directive, legal requests, and public records requests or for other business purpose.
2. Only Department Directors or higher may request monitoring of City administered IT systems for employees under their supervision for administrative purposes. Unauthorized monitoring or reading of electronic communications systems or their contents violates this Directive.
3. Any request to monitor must be approved by the CIO or his/her designees as well as the Human Resources (HR) Director or higher.
4. To obtain the necessary authorization, a written request from the requestor's Department Director to the HR Director must include subject employee information (i.e. name, employee number), a specific description of request (e.g. Email, share drives, web usage, telephone call logs and voice mail, etc.) and name and phone number of the employee in the requesting department who is responsible for coordination of the request.

The HR Director will forward the request to the CIO or designees for concurrence as well as to assign staff from ITSD to assist as necessary with any monitoring activities.

Roles & Responsibilities

Users	1. Users are required to adhere to the provisions of this AD. 2. Users should be aware that all information created, stored, or processed by a COSA information technology system is the property of the City of San Antonio. There should be no expectation of user privacy or confidentiality with regard to any files, including Email, stored on City computers. Any materials stored or processed on City information systems may be monitored and reviewed by City management at any time. In addition, users should be aware that any information processed and/or stored on any City information technology system is subject to applicable open records laws. 3. All lost equipment must be reported to the ITSD Service Desk. All stolen IT equipment shall be reported to the San Antonio Police Department (SAPD) and the associated case numbers reported to the ITSD Service Desk. COSA IT equipment can be any City-owned device, mobile device, and/or personal device that contain COSA data. In addition, all COSA capital assets that are lost or stolen shall be reported to the Finance Department in accordance with A.D. 8.7. 4. Users who voluntarily terminate employment or contract, retire, or are transferred, will be required to review their e-mail accounts with their supervisor or sponsor. The user's supervisor or sponsor is responsible for ensuring that e-mail records are properly classified and stored. All unnecessary working or convenience copies shall be disposed of appropriately.

ITSD	1. ITSD and Human Resources will provide City departments with initial communication and training regarding application of this directive. However, City Department Directors are ultimately responsible for communicating the policies established in this AD to all personnel in their respective departments and for ensuring compliance within their respective departments. 2. ITSD is responsible for publishing and disseminating the standards and procedures established to implement this directive to all relevant personnel, third-party users including (contractors, consultants, vendors, business partners etc.) and for monitoring compliance. City departments who work with third-party users are responsible for identifying the third-party users to ITSD upon on boarding and terminating. 3. ITSD is responsible for ordering, inventorying, managing, and supporting all of the City's information technology assets, which includes, but not limited to, desktops, laptops, tablets, mobile phones, servers, software, mobile applications, networking equipment, and printers. 4. Any computer-based device may be disconnected from the City network at any time, if continued connectivity constitutes a threat to the City or any City-administered information technology system. ITSD will attempt to contact the business owner responsible for the computer prior to disconnecting as long as such notification does not allow further degradation of the City-administered information technology systems. Such notification will be made after the disconnection, if prior coordination was not possible. 5. User's access may be terminated if he/she is found in breach of this directive. Service may be restored to the user following a written request by the user's Department Director or sponsor. 6. ITSD may isolate a sender's email message from reaching a user's City e-mail account. The following process must be followed in order to isolate email messages sent to the City's email system: 7. A user who receives repeated or multiple unsolicited, unacceptable annoying, alarming, abusive, embarrassing or offensive e-mail messages from a sender outside of the City must request the sender to stop sending such messages and inform the sender that any emailed requests for City records or documents must be sent to the City's Officer for Public Information at: http://www.sanantonio.gov/opengovernment. 8. The user must provide copies of the messages and all correspondence between the user and sender, to the user's Department Director or appropriate Executive Leadership Team (ELT) member along with a written request to have ITSD isolate the sender's e-mails. 9. The Department Director or ELT member and the Office of the City Attorney will review the request and determine if the request is warranted. 10. It the request is deemed warranted and subsequently approved, it will be submitted to ITSD Customer Service for email isolation. 11. ITSD will work with Human Resources to provide a security awareness training program annually to City employees.

Department Directors and their Designees	1. Departments are responsible for implementation, training, and enforcement of the data classification standards defined by the Texas State Attorney General's Office as they apply to information created, stored, or processed on City-administered technology or equipment including data retention and disposition. 2. Department Directors are responsible for any disciplinary actions taken against employees who violate this policy. The Human Resources Department will provide guidance as required to City departments regarding appropriate disciplinary actions to be taken against employees who violate this policy. 3. Department Directors/designee are responsible for requesting all IT services and equipment including, desktop computer, laptop, tablet, mobile phone or other mobile IT equipment as well as access to non-departmental data. 4. IT assets requested by Department Directors will be assigned to the department in the COSA asset management system. Director/designee and the user receiving equipment will be required to complete all necessary forms accepting accountability for equipment and will be responsible for use and protection of asset. 5. Upon the voluntary or involuntary termination of any department employee or non-employee with system or physical access, or upon notification of such termination, the Department will notify HR and ITSD to ensure access authorizations are revoked. Department will take custody of, or ensure the safe return, modification, or destruction of the following items assigned, or relating, to the terminating or notified person: • Keys, parking passes/cards, and identification badges. • Change lock combinations and passwords that would have been used by terminated user on department managed systems not accessed through their network password. • Collect sensitive documentation, along with operator procedures, and other documentation and manuals. • Notify ITSD prior to any reassignment of COSA owned computers, mobile devices, software or other IT assets. 6. Department Directors will be provided a biannual departmental IT equipment inventory for discrepancy reconciliation.
Office of the City Clerk	1. The Records Management Officer will, in cooperation with ITSD, ensure that appropriate training and communication, retention, maintenance, and disposition requirements for applicable information are in accordance with AD 1.34 Paper, Microfilm, and Electronic Records Management. 2. Responsible for the creation, maintenance and administration of all rules regarding the classification and protection of applicable information stored on City-administered information technology systems.

Human Resources	1. Human Resources Department is responsible for providing accurate job descriptions and requiring security responsibilities to be addressed in the terms and conditions of employment. Candidates for employment will be adequately screened, especially for positions of trust. Furthermore, management will require employees, contractors and other users, to apply security in accordance with established policies and procedures. 2. Human Resources will provide guidance to department for disciplinary actions associated with violations of the directive. 3. Human Resources will assist ITSD in providing training regarding this directive to current and future employees. New employees are provided a copy of this directive and users with network and application access are enrolled in security awareness training which includes an acknowledgment regarding the acceptable use of COSA technology. 4. The HR Director will consult with the Chief Information Officer (CIO) or his/her designee in approving any monitoring of systems for personnel administration purposes.

Discipline

Compliance with COSA administrative directives, security policies, and/or procedures is the responsibility of all COSA employees, contractors and/or other third parties. The City can temporarily or permanently suspend, block, and/or restrict access to information or physical assets, independent of such procedures, when it is reasonable and associated probable cause exists to do so in order to protect the confidentiality, integrity or availability of City resources as well as protect the City from liability, and/or to comply with applicable federal, state, and municipal laws, regulations, statutes, court orders, or other contractual obligations. Violations of any of these directives shall result in disciplinary actions in accordance with section 2 of Rule XVII of the Municipal Civil Service Rules for civilian employees, or in accordance with Chapter 143 of the Texas Local Government Code and current respective Collective Bargaining Agreement for uniformed employees covered under collective bargaining agreements. Administrative action may range from reprimand and loss of access privileges to suspension to separation of employment. Violations may also result in civil and/or criminal prosecution.