CITY OF SAN ANTONIO

Administrative Directive	**7.8d Access Control**
Procedural Guidelines	Controlling Access to City Systems
Department/Division	Information Technology Services Department (ITSD)
Effective Date	June 01, 2013
Revisions Date(s)	December 14, 2017
Review Date	Apr 2, 2021
Owner	Patsy Boozer, CSO

Purpose

This Administrative Directive (AD) provides a framework for controlling access to the City of San Antonio's (COSA) information assets. It identifies requirements and responsibilities needed to properly manage access control, helping to ensure the confidentiality, integrity and availability of City system(s). This directive supersedes 7.8c on Remote Access, 7.8d on Account Access Management and 7.8e on User Account Management.

This directive is designed to help control logical and/or physical access to COSA information assets. COSA is subject to federal and state regulations and/or requirements that govern access control requirements (i.e. tax record laws/regulations, public records, Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Criminal Justice Information Services (CJIS) policy for Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA), Payment Card Industry (PCI), etc.).

Controlling access to COSA systems prevents unauthorized access; limits access to sensitive resources; and restricts users to performing functions that are within the scope of their authority and/or responsibility. Access controls also assist in controlling the kinds of data, transactions, operations and activities that may be performed on COSA IT Systems. Appropriate access controls provide reasonable assurance and user accountability that access attempts, actions taken and transactions committed may be associated with a specific individual. Access Controls also pertain to the proper classification and protection of physical and logical diagrams, personnel listings, operations manuals, and IT system configuration information among other data. Improper access controls within units and departments can reduce the reliability and integrity of computerized data as well as increase the risk of data destruction, unauthorized program changes and/or other inappropriate disclosure of data. Should confidential information be disclosed, it could result in unnecessary vulnerabilities to the COSA environment.

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, Partners and Other Third Parties

Definitions

Access	The ability to do something with a computer resource (use, change, or view).
Access controls	A manual or automated mechanism by which a system grants or revokes the right to access some data, or perform some action. Access controls are the means by which the access ability is explicitly enabled or restricted in some way and they enforce segregation of duties. Access controls can be onsite via local network, offsite via remote network and/or physical access by token or badge.
Authorization	The mechanism by which a system determines what level of access a particular authenticated user should have to sensitive resources or data controlled by the system.
Availability	The mechanism whereby systems and networks provide adequate capacity in order to perform in a predictable manner with an acceptable level of performance.
Confidentiality	Ensuring that the information and processing capabilities of City information assets are protected from unauthorized disclosure or use.
Identification	The process whereby a network element recognizes a valid user's identity.
Information Systems	Computer(s), hardware, software, storage media, and network(s); the procedures and processes used to collect, process, store, share or distribute information by and through the City's computing and network infrastructure.
Integrity	Ensuring that information held on information systems is not subject to malicious or accidental alteration and that system processes function correctly and reliably.
IT Resources	Any IT related or physical resource associated with IT such as IT infrastructure, databases, networks and software packages and applications.
Least Privilege	An access control principle requiring that a computer user be given only the level of access needed to perform their job duties.
Network	A group of two or more computers linked together to facilitate communication, data sharing and processing among other computer activities.
Segregation of duties	The process of segregating work responsibilities to help ensure critical stages of a process is not under the control of a single individual.
User	Any employee or non-employee who uses COSA-administered information assets and/or system(s), exclusive of COSA’s web pages.

Policy

- COSA is required to implement, access and apply security controls, including access control(s) to protect sensitive and regulated data by Federal and state laws/regulations, as well as industry standards (e.g. Payment Card Industry)
- The National Institute of Standards and Technology (NIST) Cyber Security Framework based on 800-53 Security Controls and industry best practices have been adopted by COSA

to provide a protection framework for maintaining the confidentiality, integrity and availability of COSA systems and data.

- Organizational responsibility for the development, implementation, maintenance and/or compliance monitoring of this directive is placed with the Information Technology Services Department (ITSD).
- All information generated by and/or stored in COSA information technology systems are the property of COSA.
- Access to COSA's information and IT resources must conform to all administrative directives and ITSD security requirements.
- Access authorization should be formal, well-defined, documented and an auditable process.
- Access to COSA assets is based on an individual's membership in a group, job function and/or role in their assigned City department. Access permissions will use the principle of least privilege. All other access requires justification and approval.
- Logical and physical access controls implemented should be risk-based. Once access controls are implemented, they must be audited at least on an annual basis.
- A unique identifier and authenticator must be established for each individual (i.e., user ID) or process requesting access to COSA IT Systems.
- Where technically feasible and appropriate, access controls will enforce segregation of duties.
- COSA departments are responsible for non-employee and special account sponsorship and compliance with ITSD established provisioning and de-provisioning procedures.
- Remote access to COSA resources must comply with Human Resource (HR) and ITSD established provisioning and de-provisioning procedures.
- COSA Departments are responsible for ensuring compliance to this Directive.
- ITSD is responsible for monitoring compliance with this Directive.

This directive applies to:

- All information technology systems procured with COSA funds and/or used in the conduct of COSA business.
- All technology users who access COSA networks, data and/or applications including employees, contractors, consultants, vendors, partners and/or other third parties.
- All electronic messaging, equipment and technology that are owned or administered by the City including computers, mobile devices or personal devices reimbursed through COSA stipends (*A.D. 7.9*).
- All software, applications and/or, information system(s) developed by City personnel with City funds or licensed to the City.
- All data processed, stored and/or transmitted by a City Information Technology System(s).
- All data residing on 'Bring Your Own Devices' (BYOD) that use the COSA network.
- All remote access to the COSA network.

- All information collected or maintained by or on behalf of the City as well as all information assets used or operated by a City employee, a City contractor, a City vendor, or any other organization on behalf of the City.

Business Requirements for Access Control

- Users requesting physical access to a City facility controlled by an access control system or logical access to an information system must have completed the HR new employee or COSA third party sponsorship, background check, and attestation process.
- Local, physical and/or remote access to information resources must be explicitly approved through the user provisioning and de-provisioning, account access and/or the COSA ID request process.
- All access to the COSA network shall utilize ITSD approved technologies.
- Local, physical and/or remote access controls will be periodically reviewed for validity by ITSD, COSA department(s) and or application owners.

Non-Employee Access Requirements

To obtain local, physical and/or remote access to COSA IT resources, all third party non-employees (contractors, vendors, partners and consultants) must:

- Be sponsored by a City Department Business Owner through the non-employee provisioning process.
- Utilize defined user accounts that are only active during the individual's expected period of work or 90 days, whichever is shorter. Third party accounts not used for 90 days without prior notification will be disabled.
- The sponsoring Department is responsible for notifying Human Resources by submitting an SAP withdrawal/termination when a non-employee is no longer supporting their department.

User Access Management and Responsibility

- No individual shall engage in any activity which attempts to compromise COSA information assets or data regardless of intent.
- Any attempt to bypass or disable security controls or measures to gain unauthorized access to COSA IT assets or data is expressly forbidden.
- Departmental Data Owners are responsible for authorizing access to information.
- Access to COSA IT assets must be disabled upon separation of the employee.
- Accounts for individuals who are in a Leave of Absence (LOA) status must be disabled on the first date of absence and for the duration of the leave.
- All COSA Information Systems must be periodically screened for inactive accounts. Accounts will be disabled after 90 days of continuous inactivity or as soon thereafter as technically feasible.

Roles & Responsibilities

Employees	• Must follow the policy provided in this directive for all physical and logical access to COSA owned facilities, networks, systems and/or applications. • Must notify the ITSD Service Desk with any concerns regarding unauthorized physical or logical access to COSA owned facilities, networks, systems and/or applications.
Departments	• The Department Business System Owner is responsible for ensuring that appropriate access controls have been developed and documented in accordance with this AD. • Must Complete a COSA third party sponsorship process for any sponsored users. • Must notify HR and ITSD when a sponsored user is no longer providing support.
ITSD	• Maintains the user processes required for physical access and COSA domain user accounts. • Provisions and de-provisions access based on Departmental Business Owner authorization and approval. • Reviews and monitors data center access and domain user accounts. • Supports review process for Departmental physical and logical access controls. • Responsible for developing and maintaining an implementation standard and monitoring compliance for this directive for business systems under management control. • Responsible for working with HR to publish and disseminate the policies, standards and procedures which implement and enforce this directive.
Human Resources	• Provides support for the COSA third party sponsorship process for any sponsored users including provisioning or de-provisioning in SAP. • Support a periodic review of SAP third-party accounts that were suspended based on the ITSD 90-day inactivity review.