



City of San Antonio

Information Technology Services Department

Policy #: 7-9000-S.003 v1.5

Information Security Operational Controls Policy

Planned Effective Date: May 14, 2010

Policy Owner: John Byers (207-2206)

Policy and Standards Manager: Alan Smith (207-0547)

Replaces and Supersedes: New

Document Status	Document Number	Published Date	Action Required	Due Date
First Draft	v. 1.3	04/12/10	Review/Provide Feedback	04/27/10
Second Draft	v. 1.4	05/04/10	Review/Provide Feedback	05/11/10
Final Version	v. 1.5	05/14/10		

TABLE OF CONTENTS

SECTION 1 POLICY SUMMARY..... 3

1.1 PURPOSE 3

1.2 GENERAL POLICY STATEMENT 3

SECTION 2 GENERAL GUIDELINES..... 4

2.1 USER SECURITY 4

 2.1.1 Staffing Process 4

 2.1.2 User Account Administration..... 5

2.2 SECURITY INCIDENT REPORTING 6

 2.2.1 Security Incident Standards 6

 2.2.2 Reporting Procedures 6

2.3 EDUCATION AND TRAINING 7

2.4 INFORMATION ASSET SUPPORT PROCESSES 7

 2.4.1 Information Asset Protection 7

 2.4.2 Configuration Management 7

 2.4.3 Backup and Transmittal..... 7

 2.4.4 Maintenance..... 7

2.5 PHYSICAL SECURITY 8

2.6 CONTRACTOR, VENDOR, AND PARTNER SECURITY 8

 2.6.1 Contractor Personnel Security 8

 2.6.2 Legally Binding Agreements 8

APPENDIX A: INFORMATION SECURITY GLOSSARY 9

Section 1 Policy Summary

1.1 Purpose

The purpose of this policy is to protect City information assets through the implementation of operational controls. The following policy defines the required behavior expected by City employees and those given access to the City's information assets.

1.2 General Policy Statement

All City information assets shall be protected from unauthorized access, use, disclosure, duplication, modification, diversion, or destruction – whether accidental or intentional – in order to maintain their confidentiality, integrity, and availability.

Pursuant to City Administrative Directive (AD) 7.8.1, *Information Security Program*, the City shall develop and implement operational controls for its information assets as they are defined in IT Policy 7-9000-S.001, *Information Security Asset Classification*. Operational controls define the behavior expected of City employees and those given access to the City's information assets. These operational controls shall include, but are not limited to:

- User Security
- Security Incident Reporting
- Education and Training
- Information Asset Support Processes
- Physical Security
- Contractor, Vendor, and Partner Security

Section 2 General Guidelines

2.1 User Security

2.1.1 Staffing Process

The City's staffing process shall involve, at a minimum, the following steps, which apply equally to all users of the City's information assets:

Step 1: Define the position

Departments shall identify and address security issues early in the process of defining a position. Once a position has been broadly defined, the responsible supervisor shall determine the type of information access needed for the position. Two general security rules shall apply when granting access to information assets:

- *Separation of duties.* The City shall divide roles and responsibilities so that a single individual cannot subvert a critical function. For example, in financial systems, no single individual shall normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment.
- *Least privilege.* The City shall grant users only the access needed to perform their official duties.

Step 2: Determine the position sensitivity

Supervisors, with assistance from the Information Technology Services Department (ITSD) and the Human Resources (HR) department, shall analyze positions and document them with a Position Sensitivity Level Designation (PSLD).

Position Sensitivity Level shall be classified as:

- *Level 1 (Non-sensitive)* – positions that include mostly low risk, non-sensitive, and non-security program responsibilities.
- *Level 2 (Moderate Risk)* – positions that require clearance for access to confidential information assets (e.g., personally identifiable information (PII), payment card industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), or other information that has been classified confidential.
- *Level 3 (High Risk)* – positions that involve the public trust and require a high degree of integrity with public confidence in the individual occupying the position.

Department Directors, or their designees, shall approve the PSLD for the positions in their organizations.

Step 3: Designate the following positions as no lower than “Moderate Risk”

- Executive-level information security liaisons and their alternates
- Individuals who have either programmer privileges or have the ability to establish access to information assets that process confidential data

Step 4: Update each job description to reflect its security responsibilities and sensitivity level

“Security responsibilities” refer to employee obligations to protect information assets according to their classification and security controls and to use such assets only in the execution of official duties.

Step 4: Ensure that all other individuals with access to City information assets (e.g., contractors, volunteers) meet the requirements of City employees performing similar duties

Step 5: Use the HR background check process as required by the security level and risk of the position

The ITSD Chief Technology Officer (CTO), or his designee, shall issue “Security and Risk Designation” guidelines that shall define risk levels and their corresponding security investigation requirements with regard to position sensitivity designations.

Step 6: Conduct regular employee training and awareness

In coordination with ITSD, departments shall train their employees in the computer security responsibilities and duties associated with their jobs.

2.1.2 User Account Administration

Per *Administrative Directive (AD) 7.8D – Account Access Management* and *AD 7.8E – User Account Management*, departments, in cooperation with ITSD, shall ensure the effective administration of their users’ access to information assets in order to maintain necessary security levels. Access requirements to information assets by third parties, contractors, and vendors must meet those requirements established for comparable departmental employees.

Departmental managers and supervisors, or their designee(s), shall sponsor access for all their users, including non-departmental users. A signed request for user access by management, or their designee(s), constitutes management approval to initiate a request for access to any information asset. The request shall contain the user’s name, requesting organization (or name of contracting company and contract number if applicable), work location, purpose for access, access required, and any other information deemed necessary by ITSD.

Each department shall ensure that user access and privileges are reviewed at intervals appropriate to the sensitivity levels and security responsibilities of a position. The maximum interval shall not exceed one (1) year. Reviews shall examine the levels of access for each individual, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up to date, and whether required training has been completed.

Access authorizations are typically changed in two types of circumstances:

- Change in job role, either temporarily (e.g., while covering for an employee on sick leave or training a new employee) or permanently (e.g., in-house transfer)
- Termination

Changes in job roles, terminations, and terminations of access shall be defined and governed by policies published by ITSD and HR, as appropriate.

2.2 Security Incident Reporting

2.2.1 Security Incident Standards

An incident refers to a computer security problem arising from a threat. Computer security incidents can range from a single virus occurrence to an intruder attacking many networked systems, or such things as unauthorized access to sensitive data and loss of mission-critical data.

Information security incidents shall be categorized as follows (these types of acts are not all-inclusive):

- Circumvention of information security controls, safeguards, and/or procedures
- Unauthorized access, use, disclosure, alteration, manipulation, destruction, or other misuse of information assets
- Theft, fraud, or other criminal activity committed with the aide of information assets
- Theft, loss, or vandalism of hardware or software
- Issues affecting confidentiality, integrity, and availability of data
- Unauthorized downloading or copying of confidential City information

ITSD shall constitute an information security Incident Response Team (IRT) to investigate and respond to information security incidents and involve the appropriate level of law enforcement for such incidents, as necessary.

2.2.2 Reporting Procedures

The person observing or discovering the information security incidents, as defined above, shall advise his supervisor as soon as possible. Those incidents that are determined to affect the City's capability to accomplish critical functions, restrict the availability of an information asset or communications medium, or result in a monetary impact to the City, shall be reported to ITSD within two (2) hours of its discovery.

Reportable information security incidents shall be recorded on a security incident log as developed by ITSD. Incident report information shall be treated as confidential information and safeguarded as necessary, as allowed under Texas law.

2.3 Education and Training

Information security training is required for:

- New employees within 60 days of hire
- All users of City information assets on an annual basis

Information security education and training will be provided by ITSD and HR and is required for access to City information assets. Successful completion of information security education and training shall be documented as required by HR.

2.4 Information Asset Support Processes

2.4.1 Information Asset Protection

Per *AD 7.5 – Acceptable Use of Information Technology*, departments and users shall protect all City information assets, such as computers and peripherals, communication devices, media, and software, against theft and unauthorized use.

2.4.2 Configuration Management

All City information assets shall employ configuration management at a level commensurate to the size, complexity, and sensitivity of the information asset. Configuration management provides a complete audit trail of change decisions and design modifications to the asset. The City shall perform configuration management to:

- Manage changes made to an information asset throughout its lifecycle
- Identify and document the functional and physical characteristics of an information asset, record its configuration, and control changes to it and its documentation
- Ensure that changes to the asset do not unintentionally or unknowingly diminish required security controls

ITSD shall define the configuration management process and standards for City information assets.

2.4.3 Backup and Transmittal

The City shall ensure that backups or copies of information assets, such as data, deploy and maintain the same level of security controls as used for the operational asset. Physical protection of media shall be extended to backup copies stored offsite. Backup copies shall be accorded an equivalent level of protection to media containing the same information stored onsite. Equivalent protection, however, does not mean that the security measures need to be the same. The controls at the off-site location are quite likely to be different from the controls at the regular site. Information assets transferred within a facility or to outside areas shall be secured during transmittal in accordance with its classification and required security controls.

2.4.4 Maintenance

ITSD shall publish guidelines to ensure that only authorized personnel perform maintenance of information assets. Technical support and maintenance work performed at City facilities (on-site) shall be supervised by or under the control of the City personnel knowledgeable about the information asset's operations.

Automated or remote diagnostic maintenance of confidential City assets with outside vendors is prohibited unless authorized by the asset's accreditation. If authorized, authentication of the maintenance provider prior to access is required. Factory-set passwords shall be changed or otherwise disabled until they are needed.

2.5 Physical Security

Staff and equipment require a safe, secure, and technically sound physical environment. ITSD shall promulgate guidelines and standards for the physical security of City information assets. Information asset owners shall ensure that all their assets are protected as required by the assets classification (see *7-9000-S.001 Information Security Asset Classification Policy*) and the guidelines and standards established by ITSD.

2.6 Contractor, Vendor, and Partner Security

2.6.1 Contractor Personnel Security

Information security requirements and specifications for third party or vendor personnel contracted from commercial sources shall be defined and incorporated into all contractual agreements prior to execution. Contractors and their employees shall be granted limited and controlled access to information assets consistent with established security requirements.

Contractor access to the City's confidential information assets must be in the interest of the City. Access shall be limited to a specified timeframe and then reviewed for possible termination. Departmental executives must officially sponsor all non-City personnel accessing City information assets. Contractors shall receive the same security training required for City employees, including orientation and periodic security updates. Contractors shall indicate in writing that they have read, understand, and will comply with the City information security requirements applicable to them.

2.6.2 Legally Binding Agreements

All City information security requirements for the acquisition, maintenance, or operation of City information assets shall be included in all legally binding agreements, including, but not limited to, contracts, sharing agreements, inter-local agreements (ILA), statements of work (SOW), and memoranda of understanding (MOU). These legally binding agreements shall be reviewed by the appropriate executive-level information security liaison for security implications prior to the execution of the contract. A separate section in the legally binding agreement dealing with security issues shall be incorporated, where appropriate. Access to the City's information assets by third party or vendor personnel in the performance of their agreed upon duties shall be outlined in the legally binding agreement, as necessary.

Appendix A: Information Security Glossary

<i>Access Control</i>	Security control designed to permit authorized access to an IT system or application.
<i>Accreditation</i>	Authorization by the Information Technology Services Department (ITSD) Chief Technology Officer (CTO), or designee, to place an IT system into operation.
<i>Audit Trail</i>	A record showing who has accessed a computer system, when, and what operations he or she has performed during a given period. Audit trails are useful both for maintaining security and for recovering lost transactions.
<i>Authentication</i>	The process of determining whether someone or something is, in fact, who or what it is declared to be.
<i>Availability</i>	Ensuring that information systems, including stored information and processing capability, are always available to authorized users when needed.
<i>Backup</i>	A copy of data and/or applications contained in the IT stored on magnetic media outside of the IT to be used in the event IT data are lost.
<i>Certification</i>	The technical and non-technical evaluation of an IT system – by the system owner or by an independent certifying agent – that produces the necessary information required by the authorizing official to make a credible, risk-based decision on whether to place an IT system into operation.
<i>Ciphertext</i>	Form of cryptography in which the plaintext is made unintelligible to anyone, who intercepts it by a transformation of the information itself, based on some key.
<i>Classification</i>	A systematic arrangement of objects into groups or categories according to a set of established criteria.
<i>Commercial-Off-The-Shelf (COTS) Software</i>	Software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.

<i>Confidentiality</i>	Ensuring that the information and processing capabilities of City information assets are protected from unauthorized disclosure or use.
<i>Configuration Management</i>	The process of keeping track of changes to the system, if needed, approving them.
<i>Contingency Plan</i>	A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.
<i>Controls</i>	The means of managing risk, which includes policies, procedures, guidelines, practices, or organizational structures. Controls may be management (e.g., risk management plan), operational (e.g., strong password rules), or technical (e.g., corporate firewalls) in nature.
<i>Corrective Actions</i>	Steps that are taken to address existing nonconformities and make improvements. Corrective actions deal with actual nonconformities (problems), ones that have already occurred. They solve existing problems by removing their causes. In general, the corrective action process can be thought of as a problem solving process.
<i>Data</i>	Information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data. Computer data may be processed by the computer's CPU and stored in files and folders on the computer's hard disk.
<i>Degaussing Media</i>	Method to erase data from magnetic tape magnetically.
<i>Document</i>	A form of information. A document can be put into an electronic form and stored in a computer as one or more files. Often a single document becomes a single file. An entire document or individual parts may be treated as individual data items. As files or data, a document may be part of a database.
<i>File</i>	A collection of data stored in one unit, identified by a filename. It can be a document, picture, audio, or video stream, data library, application, or other collection of data.
<i>Friendly Termination</i>	The removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable.
<i>Gateway</i>	A bridge between two networks.

<i>Hardware</i>	Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips.
<i>Information Asset</i>	All records, documents, data, and systems created, owned, or managed by the City.
<i>Information Asset Owner</i>	A person or group of people with authority and responsibility for establishing the controls for an information asset's generation, collection, processing, dissemination, and disposal.
<i>Information Security</i>	Measures taken to preserve the confidentiality, integrity and availability of information; ensures that information is authentic, reliable, and from an accountable source.
<i>Information Security Plan</i>	Document that details the security controls established and planned for a particular system.
<i>Information System</i>	Computers, hardware, software, storage media, and networks; the procedures and processes used to collect, process, store, share or distribute information by and through the City's computing and network infrastructure.
<i>Information System Administrator</i>	The individual responsible for defining the system's operating parameters, authorized functions, and security requirements. This individual is usually the person who maintains the system on a day-to-day basis.
<i>Information System Owner</i>	The individual who is ultimately responsible for the function and security of the system.
<i>Integrity</i>	Ensuring that information held on information systems is not subject to malicious or accidental alteration and that system processes function correctly and reliably.
<i>Intrusion Detection</i>	Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
<i>Issue-Specific Policy</i>	Policies developed to focus on areas of current relevance and concern to an office or facility. Both new technologies and the appearance of new threats often require the creation of issue-specific policies (e.g., e-mail, Internet usage).

<i>IT Security</i>	Measures and controls that protect an IT against denial of and unauthorized (accidental or intentional) disclosure, modification, or destruction of IT systems and data. IT security includes consideration of all hardware and/or software functions.
<i>IT Security Policy</i>	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
<i>Least Privilege</i>	The process of granting users only those accesses they need to perform their official duties.
<i>Local Area Network</i>	A short-haul data communications systems that connects IT devices in a building or group of buildings within a few square miles, including (but not limited to) workstations, front-end processors, controllers, switches, and gateways.
<i>Management Controls</i>	Security methods that focus on the management of the computer security system and the management of risk for a system.
<i>Network</i>	Two or more systems connected by a communications medium; a network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.
<i>Operating System</i>	The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.
<i>Password</i>	Protected/private character string used to authenticate an identity or to authorize access to data.
<i>Port</i>	An interface on a computer to which you can connect a device.
<i>Port Protection Device</i>	A device that authorizes access to the port itself, often based on a separate authentication independent of the computer's own access control functions.

<i>Preventive Actions</i>	Steps that are taken to avoid potential nonconformities and make improvements. Preventive actions address potential nonconformities (problems), ones that have not yet occurred. Preventive actions prevent the occurrence of problems by removing their causes or reduce the likelihood that they will occur. In general, the preventive action process can be thought of as a risk management process.
<i>Private Branch Exchange (PBX)</i>	A private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.
<i>Record</i>	Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. Record definitions for the City of San Antonio are contained in COSA Administrative Directive 1.34.
<i>Remote Access</i>	The hookup of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information
<i>Risk</i>	The possibility that an event that will adversely impact the City's information assets. The potential risk is measured by the cost of the risk to the City, if realized, discounted by the probability, or the likelihood, that the risk will occur.
<i>Risk Assessment</i>	A process to identify, analyze, and manage potential risks.
<i>Risk Management</i>	Process of identifying, controlling, and eliminating or reducing risks that may affect IT resources.
<i>Sensitive Information</i>	Any information, the loss or misuse of which could adversely affect the privacy to which individuals are entitled.
<i>Sensitivity</i>	A measure of the importance assigned to information by its owner, for denoting its need for protection.
<i>Software</i>	Computer instructions or data. Anything that can be stored electronically is software.
<i>Technical Security Policy</i>	Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the IT product in supporting the information protection policy control objectives and countering expected threats.

<i>Telecommunications</i>	Any transmission, emission, or reception of signals, writing, images, sound or other data by cable, telephone lines, radio, visual or any electromagnetic system.
<i>Threat</i>	Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial thereof.
<i>Trojan Horse</i>	Any program designed to do things that the user of the program did not intend to do, or that disguise its harmful intent. A program that installs itself while the user is making an authorized entry; and, then is used to break-in and exploits the system.
<i>User</i>	Any person who is granted access privileges to a given IT.
<i>Virus</i>	A self-propagating Trojan horse (a program that surreptitiously exploits the security/integrity of a program), composed of a mission component, a trigger component, and a self-propagating component.
<i>Vulnerability</i>	A weakness in automated system security procedures, technical controls, environmental controls, administrative controls, internal controls, etc., that could be used as an entry point to gain unauthorized access to information or disrupt critical processing.