



City of San Antonio

Information Technology Services Department

Policy #: 7-9000-S.002 v1.3

Information Security Management 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. 1.1	04/12/10	Review/Provide Feedback	04/27/10
Second Draft	v. 1.2	05/04/10	Review/Provide Feedback	05/11/10
Final Version	v. 1.3	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 MANAGEMENT CONTROL PLANS 4

 2.2 RISK MANAGEMENT PLANS 4

 2.3 MANAGEMENT RESPONSE (CONTINGENCY) PLANS..... 5

APPENDIX A: INFORMATION SECURITY GLOSSARY 7

Section 1 Policy Summary

1.1 Purpose

The purpose of this policy is to protect City information assets through the implementation of management controls. The following policy defines the required behavior expected by those in leadership positions in the City 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 management controls for its information assets as they are defined in IT Policy 7-9000-S.001, *Information Security Asset Classification*. Management control plans are not the same as information security plans (ISP), for which the Information Technology Services Department (ITSD) is responsible. Rather, management control plans define how City departments regulate the information assets under their control, management, or responsibility. These controls focus on the management of information assets and the management of risk for those assets. This policy requires departments to create and maintain:

- Management Control Plans
- Risk Management Plans
- Management Response Plans

Section 2 General Guidelines

2.1 Management Control Plans

Departments shall develop a management control plan for any information asset used, managed, or controlled by the department, whether housed at that department or in a remote location. Information assets are defined in IT Policy 7-9000-S.001, *Information Security Asset Classification*. Each department shall:

1. Assess department-level information asset risks
2. Assign roles and responsibilities for information assets and risks
3. Identify the appropriate individuals to serve as liaisons for further information, guidance, and compliance
4. Create department-level information asset risk management plans
5. Manage the risk to department-level information assets, as appropriate

Departments shall document the above management control plans and file a copy with the Information Technology Services Department (ITSD) and the Office of Emergency Management (OEM). These documented controls shall be reviewed every five years or earlier, if required. ITSD shall publish a timeframe to classify City information assets and the development of management control plans.

2.2 Risk Management Plans

2.2.1 Risk Assessments

All departments shall establish and maintain plans for conducting periodic risk assessments to ensure that appropriate, cost-justified safeguards are incorporated into existing or new information assets. The risks identified by departments should be (1) specifically defined, (2) tangible, and (3) measurable. Departments shall:

- Assess the business impacts that might result from security failures, considering the consequences of a loss of confidentiality, integrity, or availability of the assets
- Assess the realistic likelihood that security failures might occur in light of prevailing threats and vulnerabilities, the impacts associated with the assets, and the controls currently in place
- Estimate the level of risk to an information asset based upon the likelihood and impact of the risk

Per AD 7.8.1 *Information Security Program*, ITSD shall assist departments to conduct these assessments.

2.2.2 Risk Responses

Departments shall manage risks with four different responses.

- *Avoid* – change operations to eliminate the threat entirely; e.g., shut down systems where the risk exceeds the business value
- *Transfer* – shift some or all of the risk, along with ownership of the response, to a third party; e.g., insurance, outsourcing, etc.
- *Mitigate* – reduce the probability or impact of a risk to acceptable levels; e.g., implement stronger access controls
- *Accept* – take no action other than to document that the risk has been accepted and the reasons for its acceptance

If an information asset is controlled, managed, or owned by multiple departments, they may make a collective determination on how to complete the risk assessment and manage the risk. However, the departments shall designate a single point of contact (POC) to liaise with ITSD.

2.2.3 Risk Assessment Schedule

Departments shall add new risks to the risk assessment, as they are identified. Assessments shall be performed every five years or more frequently when:

- A new information asset is acquired
- Whenever there is a significant change to an existing information asset as defined by the department

Based on the results of the risk assessment, departments shall determine how to manage the risks, pursuant to the risk responses defined in [2.2.2 Risk Responses](#). Risk responses may require additional budget funding. Departments shall notify the Office of Management and Budget (OMB) to request additional funds, if necessary. Not all risks can be avoided, transferred, or mitigated due to budget constraints, staffing limitations, or an inability to transfer the risk to a viable third party. Some risks may be accepted.

2.3 Management Response (Contingency) Plans

Departments shall be responsible for the development and maintenance of management response plans. Management response plans shall include, at a minimum:

- The backup and recovery schedule of data and software (note: ITSD shall provide the service for conducting backups of data and software under its control; departments shall coordinate the details and frequency of these backups in accordance their business continuity/disaster recovery (BC/DR) plans.)
- The emergency response actions to be taken to protect information assets to minimize the impact of the risk event

- The selection of a backup or alternate operation strategy to continue business operations
- The actions to be accomplished to initiate an effective recovery of business processes including a move to an alternate site, if necessary
- The resumption of normal operations in the most efficient and cost-effective manner

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.