



City of San Antonio

Information Technology Services Department

Policy #: 7-9000-S.001 v1.4

Information Security Asset Classification 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. 1.2	04/12/10	Review/Provide Feedback	04/27/10
Second Draft	v. 1.3	05/04/10	Review/Provide Feedback	05/11/10
Final Version	v. 1.4	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 INTRODUCTION 4

2.2 SCOPE 4

2.3 INFORMATION ASSET CLASSIFICATION 4

2.4 INFORMATION OWNER 4

2.5 IMPLEMENTATION 4

2.6 IDENTIFICATION OF CONFIDENTIAL INFORMATION 9

2.7 INFORMATION ISOLATION 9

2.8 INFORMATION DISPOSAL..... 9

APPENDIX A: INFORMATION SECURITY GLOSSARY 10

Section 1 Policy Summary

1.1 Purpose

The purpose of this policy is to protect City information assets through the implementation of asset classification and controls. This policy ensures that City information assets are identified, properly classified, and protected throughout their lifecycles. This policy applies to all City employees with responsibility for and control over 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 implement information asset classification. This classification assists the management of information assets and the management of risk for those assets. Information asset classification shall include:

- Inventory of Assets
- Accountability of Assets
- Security Classification of Assets

Section 2 General Guidelines

2.1 Introduction

Information, like other assets, must be properly managed from its creation to disposal. As with other assets, not all information has the same value or importance to the City and therefore information requires different levels of protection. Information asset classification is critical to ensure that the City information assets have a level of protection corresponding to the sensitivity and value of the information asset.

All City information assets shall be classified and managed based on its confidentiality, sensitivity, value, and availability requirements. The City shall identify its information assets and their owners, and classify each information asset. Proper levels of protection shall be implemented to protect these assets relative to their classifications. This policy is subject to the limitations and conditions of all applicable Federal, state, and municipal laws.

2.2 Scope

This policy applies to any information asset (e.g., systems, applications) that is used by, or interfaces with, the City computer network or systems including any system loaned, leased, or otherwise obtained that interfaces or connects to the City's network.

2.3 Information Asset Classification

Information assets shall be classified as either public or confidential.

- *Public* – information that is collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business
- *Confidential* – information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g., the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements).

Departments shall work with the Office of the City Clerk to align with Federal, state, and municipal regulatory rules for information classification and retention.

2.4 Information Owner

All information assets shall have an information asset owner or owners established with the appropriate department, departments, or other government entities. Information asset owners may be individuals or groups of individuals that best comport with the nature of the asset.

2.5 Implementation

The information asset classification process shall adhere to the following activities and timeline:

Table 1. Information Asset Classification Timeline

Activity	Due
Information asset classification process defined and implemented	End of FY10

New are classified in detail (Begins with critical systems)	End of FY11
Legacy assets are classified in detail (Begins with critical systems)	FY11 – FY14
Processes implemented for periodic information asset reassessment and maintenance	FY15

2.5.1 Define and Implement Information Asset Process

ITSD shall develop a business process to classify information assets owned or managed by the City.

2.5.2 Identify Information Assets

Information assets come in many physical and electronic forms, and include, but not limited to:

- Documents
- Data
- Images
- Audio
- Video

Examples of information assets include, but are not limited to:

- Employee-related information including employee records, job applications, and records of interviews
- Procurement records such as RFP specifications, evaluation of proposals, contracts, pricing details, and performance reports
- City operational information such as policies, strategic plans, correspondence, legal advice, financial and audit reports, system documentation, user manuals, training material, operational and support procedures, business continuity plans, system architecture drawings, and risk analyses
- Vendor information including service level agreements, service contracts, and client contact records
- Citizen and customer information including personal identity information collected to issue licenses or certifications, building permits, and customer service requests
- Public safety and justice information, such as fields reporting data, incident reports, case data, and emergency plans

The City shall focus on identifying critical information assets first. Where practical, the City shall leverage other business initiatives such as business continuity planning/disaster recovery

planning or the implementation of enterprise policies and initiatives to identify information assets.

2.5.3 Identify Information Asset Owners

All information assets should have an identified information asset owner established. These information owners are responsible for:

- Assisting the inventory of information assets
- Assigning classification levels to all information assets
- Approving decisions regarding controls, access privileges of users, and ongoing decisions regarding information management
- Conducting, in accordance with the information asset classification schedule:
 - Periodic information asset reviews to manage changes to risk due to new threats, vulnerabilities, or changes in the business and technical environments
 - Periodic reclassification based upon business impact analysis, changing business priorities, and/or new laws, regulations, and security standards
- Following record retention rules regarding proper disposition of all information assets

Information should be classified by the information asset owner, or delegate, at the earliest possible opportunity and as soon as the owner is aware of the sensitivity of the information asset. Consideration must be given to stakeholders, users, and consumers of the information asset with regard to accessibility and business process changes that may adversely affect their respective business processes or consumer needs.

In the case of information externally generated and not otherwise classified, the City employee who receives the information asset should contact his or her department information asset owner or delegate to classify the information and guide its control within the City.

2.5.4 Conduct Risk and Impact Assessment of Information Assets

Once information assets are identified, conduct an impact assessment on the value of the asset to the organization and any risks associated with its disclosure. Include in the assessment any known legislation, regulations, policy compliance, and contractual obligations affecting the management or use of the information.

Classification decisions are not strictly limited to a consideration of the threat to security. The costs of additional steps and additional resources needed to manage the risk, cost of not managing risk, and whether there is an information exchange associated with the information asset should be considered. The City shall determine the classification level based on a balanced approach.

2.5.5 Determine Information Asset Classification

Once assets are identified and a risk assessment completed, assign information asset classifications to the assets. Information assets should be classified according to business need and findings from the impact assessment. Business needs vary and similar information assets may be classified differently from department to department. One department may classify their network diagrams as confidential and another department may classify their network diagrams as public based on the level of detail provided and the business need. If assets interconnect, they shall be classified at the highest level given. For example, if one department classifies an asset as “Confidential” and another department classifies the same asset or an interconnected asset as “Public,” then the assets shall be classified as “Confidential.” As much as possible, ITSD shall develop standard classification scheme, whereby information asset owners will know which assets must always be classified as “Confidential” and which assets may be left to their discretion.

All City information assets shall be identified by one of three levels of risk. Texas Administrative Code §202.22, Managing Security Risks, states,

“A risk assessment of information resources shall be performed and documented. The risk assessment shall be updated based on the inherent risk. The inherent risk and frequency of the risk assessment will be ranked, at a minimum, as either ‘High,’ or ‘Medium,’ or ‘Low.’

“High Risk” assets, which must be assessed annually, are information assets that:

- Involve large dollar amounts or significantly important transactions, such that business or government processes would be hindered or an impact on public health or safety would occur if the transactions were not processed timely and accurately, or
- Contain confidential or other data such that unauthorized disclosure would cause real damage to the parties involved, or
- Impact a large number of people or interconnected systems.

“Medium Risk” assets, which must be assessed biennially, are information assets that:

- Transact or control a moderate or low dollar value, or
- Data items that could potentially embarrass or create problems for the parties involved if released, or
- Impact a moderate proportion of the customer base.

“Low Risk” assets, which must be assessed biennially, are information assets that:

- Publish generally available public information, or
- Result in a relatively small impact on the population.

Once the appropriate classification is identified, the asset and its classification must be documented. ITSD shall establish and maintain a register to document the classification of each information asset. At a minimum, the register shall include:

- Name or unique identifier of asset or group of assets
- Description of information asset (i.e., what type of information it contains)
- Location of information asset
- Information asset owner
- Classification of the information asset
- Date of classification with details of the authority for the classifier (i.e., who approved the classification)
- Reason for the classification of the information asset (particularly important to support review and reclassification of the information asset at a later time; should include legislative, regulatory, policy or other reference where applicable, or a copy of the impact assessment date)
- Date to review classification

The following information is desirable in the register(s) for highly sensitive or confidential information assets:

- Users and usage of the information
- Number of copies in circulation and their location
- Disposal details where information has been disposed of

Information asset classification is not the same as certification and accreditation. Certification and accreditation is a process whereby an information asset is evaluated and approved for operation in the City because it satisfactorily functions according to its prescribed security safeguards. Information asset classification is a necessary component of the certification and accreditation process. Accordingly, while information asset classification will follow the timeline documented in this policy, formal certification and accreditation of all City information assets will take longer and depend upon available resources and funds.

2.5.6 Implement Information Security Controls

Each information asset classification shall have a set or range of controls, designed to provide the appropriate level of protection to the information asset commensurate with the value of the information in that classification.

2.5.7 Maintain Controls and Conduct Periodic Reviews

Information asset owners shall use the classification information register to review the classification of identified information assets, in accordance with a schedule determined by the classification of the asset.

ITSD shall establish practices for periodic reclassification based on business impact analysis, changing business priorities or new statutes, regulations and security standards.

ITSD shall establish procedures for adding new information types or deleting information no longer maintained by the City.

2.6 Identification of Confidential Information

Proper labeling enables all parties to correlate the information with the appropriate information handling guidelines. Information assets shall be properly labeled so that users are aware of their classification.

All Confidential assets shall have a “Confidential” classification notification. This includes databases, systems, reports, spreadsheets, letters, and memos. To the extent feasible, confidential information assets, as such, shall be identified by a means appropriate to the system or storage medium.

2.7 Information Isolation

Information belonging to different information asset classifications shall be either logically or physically separated or the aggregate information protected at the highest classification level. Whenever and wherever possible, confidential information assets should be stored in a separate, secure area.

2.8 Information Disposal

All electronic, paper, and physically recorded information assets must be disposed of in a manner consistent with the information asset classification of the information and comply with established Federal, state, and municipal laws, rules and regulations.

ITSD shall issue disposal procedures for electronic information assets, such as desktops, laptops, mobile devices, and databases.

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.