



City of San Antonio

Information Technology Services Department

Policy #: 7-9000-S.005 v1.6

Information Asset Certification and Accreditation 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. 1.4	04/12/10	Review/Provide Feedback	04/27/10
Second Draft	v. 1.5	05/04/10	Review/Provide Feedback	05/11/10
Final Version	v. 1.6	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 CERTIFICATION AND ACCREDITATION 4

 2.2 SCOPE 4

 2.3 INITIAL CERTIFICATION AND ACCREDITATION..... 4

 2.4 INTERIM CERTIFICATION AND ACCREDITATION 5

 2.5 RENEWAL OF CERTIFICATION AND ACCREDITATION..... 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 certification and accreditation (C&A). The following policy defines the requirements that ensure that all information security conditions, including all applicable Federal, state, and municipal policies, regulations, and standards, are met for all City 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 certification and accreditation for its information assets as they are defined in IT Policy 7-9000-S.001, *Information Security Asset Classification*. All information assets must include information security controls that manage the risks to those assets appropriate to the probability of those risks being realized. The City shall confirm that the implemented security controls are adequate and appropriate for each information asset being accredited. C&A or “authorization for processing” shall ensure that a particular information asset is authorized to function in an operational environment under defined and acceptable information security controls.

Section 2 General Guidelines

2.1 Certification and Accreditation

The Information Technology Services Department (ITSD) shall conduct certification and accreditation (C&A) on all information assets owned, controlled, or managed by the City. ITSD shall define and publish the requirements and standards necessary to certify and accredit any information asset. The ITSD Chief Technology Officer (CTO), or his designee, shall be the accrediting authority for all City information assets. The ITSD CTO shall accredit information assets before releasing them to production. The ITSD CTO may issue “blanket” accreditation for hardware and other devices, such as telephones, memory sticks, and PCs, or where it is not necessary to ensure security.

Certification refers to the preparation and review of an information asset’s security controls and capabilities for establishing whether it meets appropriate security requirements. *Accreditation* refers to the *positive evaluation* made on the *Certification and Accreditation Package* by the evaluation team.



Figure 1. Simple C&A Process Steps

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 Initial Certification and Accreditation

All City information assets shall be accredited. Prior to accreditation, each information asset shall undergo an appropriate technical certification evaluation to ensure that it meets all Federal, State, and municipal information security policies, regulations, and standards. All assets shall employ security controls that reflect the importance of the information processed on the asset.

The CTO, with the guidance of the Chief Information Security Officer (CISO), shall define the certification review process, including any required information and certification criteria. The CTO, with the guidance of the CISO, shall also establish a Certification Review Team (CRT) to conduct the technical certification evaluations of information assets. The CRT shall obtain input from all stakeholders and affected parties who have been involved with the information asset, including, but not limited to: the executive-level staff, the information asset owner, system administrator, software development staff, computer operations staff, business users, and other individuals and groups, as necessary.

The CTO, or his designee, shall review the certification documentation and shall either approve, thereby declaring that a satisfactory level of operational security is present, or disapprove, indicating that the level of risk has not been adequately defined or reduced to an acceptable level for operational requirements.

If disapproved, the CTO shall forward his decision to the information asset owner along with the certification packet and reasons for disapproval. If approved, the CTO shall sign a formal accreditation statement declaring that the asset is operating at an acceptable level of risk, or defining any conditions or constraints that are required for appropriate asset protection. This approval constitutes an Authority to Operate (ATO). For information assets owned by ITSD, approval shall be confirmed as acceptable by the Chief Information Officer (CIO).

2.4 Interim Certification and Accreditation

An interim authority to operate (IATO) may be granted for a fixed period not to exceed one year. This authority shall be based on an approved security plan for the information asset, including any conditions that must be met. The IATO permits the information asset to meet its operational mission requirements while improving its security posture.

2.5 Renewal of Certification and Accreditation

Information assets shall be re-accredited if major changes occur to the asset or every five years, whichever occurs first. Examples of major changes include:

- *Changes in the asset or software applications.* These include substantial changes that alter the mission, operating environment, or basic vulnerabilities of the asset. Major changes include an increase or decrease in hardware, application programs, external users, hardware upgrades, addition of telecommunications capability, changes to program logic of application systems, or relocation of system to new physical environment or new organization. Minor changes such as, replacement of similar hardware when capacity does not significantly change, addition of two or three workstations on a network or small modifications to an application program (e.g., table headings are changed) would not require re-accreditation.
- *Changes in protection requirements.* These include changes in the classification of the data processed by the asset, increases in the mission criticality of the asset, or changes in Federal, state, or municipal regulations, policies, or standards.
- *Occurrences of a significant violation.* These include violations or incidents that question the adequacy of existing security controls.
- *Audit or evaluation findings.* These include findings from any security review that identify significant unprotected risks. These could include the security verification review, physical or information security inspection, internal control reviews, or internal or external audits.

The information included in certification documentation may contain sensitive details about the asset. Such details may identify weaknesses or vulnerabilities that require protection against

ITSD Policy 7-9000-S.005 v1.6 Information Asset Certification and Accreditation Policy

Effective Date: May 14, 2010

Revision Date(s): None

disclosure to persons without the need to know. Accreditation documentation for confidential assets must be secured and marked “Confidential.”

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.

ITSD Policy 7-9000-S.005 v1.6 Information Asset Certification and Accreditation Policy

Effective Date: May 14, 2010

Revision Date(s): None

<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.

ITSD Policy 7-9000-S.005 v1.6 Information Asset Certification and Accreditation Policy

Effective Date: May 14, 2010

Revision Date(s): None

<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).

ITSD Policy 7-9000-S.005 v1.6 Information Asset Certification and Accreditation Policy

Effective Date: May 14, 2010

Revision Date(s): None

<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.

ITSD Policy 7-9000-S.005 v1.6 Information Asset Certification and Accreditation Policy

Effective Date: May 14, 2010

Revision Date(s): None

<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.

ITSD Policy 7-9000-S.005 v1.6 Information Asset Certification and Accreditation Policy

Effective Date: May 14, 2010

Revision Date(s): None

<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.