COIT Security Policy

Introduction

Under the provisions of the City and County San Francisco administrative code, technology and information resources are the strategic assets of the City and County of San Francisco that will be managed at the direction of the Committee on Information Technology (COIT).

Thus this initial policy is established to outline the Security Policies and guidelines for the management of City and County San Francisco technology and information assets.

Purpose

The purpose of the COIT Security policy is to inform user's staff and managers of their responsibilities, obligations and requirements for protecting the City & County of San Francisco's technology and information assets. These Security Policies should be evolving and frequently updated and addressed. The purpose of these policies should also be directed to specify mechanisms through which the policies and requirements can be met. The purpose of the policies will also be to help establish security frameworks, metrics, and governance and audit/reporting processes.

Policy

General Policy

- Governance by Executive Directive 07-09.

Security Policy

Recommends an initial policy to address the following:

- ***Create IT Security working group***. Under the direction of a COIT appointed DTIS CISSP certified Security Manager an IT Security working group will be created. This will be a DTIS and cross departmental workgroup chaired by the committee.

- ***Adopt a Security Policy Framework.*** COIT will initially adopt the California Counties Information Services Directors Association (CCISDA) Best Policies for the Countywide Information Security Program Framework (pdf) as a starting point and initial reference for CCSF Security Policies. This framework outlines security policies in the following areas: Acceptable Use, Business Continuity, Development Life Cycle, E-mail, Incident Response, Information Classification, Logon Banner, County Information Security, Password Policy, Perimeter Policies, Physical Security, Privacy and Confidentiality, Remote Access, Risk Assessment, Security Awareness Training and Education, Software & Copyrights and Virus Protection.

- ***Development and adoption of a Risk Assessment Policy***. Under the direction of the IT Security working group the departments need to identify and authorize individuals charged with the responsibility of accessing and reporting on security risks. Identify the security policies and procedures to be enforced in order to initiate appropriate remediation and perform information risk assessments for the purpose of determining areas of vulnerability.

- ***Identify and recommend Security Budget Guidelines.*** Each department shall identify and set aside an amount of funds that will or maybe needed for their department's to address issues identified as the highest risk opportunity as determined through a risk assessment process.

- The IT Security working group will define and keep current a list of job skills and functions so that departments may properly staff, or identify resources to preserve and maintain departmental information security.