Information Security Policy
City and County of San Francisco

City and County of San Francisco Technology Acceptable Use Policy

Issue Date:

Revision Date:

1. Policy Purpose

The purpose of this policy is to protect City and County of San Francisco employees, partners, and departments from illegal or damaging actions by individuals, through intentional or unintentional means, by outlining the acceptable use of all City-owned or leased computer equipment. Inappropriate use of equipment exposes the City to risks including virus attacks, compromise of network systems and services, breach of confidentiality, and legal liability.

2. Policy Scope

This policy applies to all employees, interns, volunteers, or any other City workers, contractors and vendors, and to any person or agency with access to City computers. This policy applies to all equipment owned or leased by the City.

3. Departmental Responsibilities

Departments are responsible for the enforcement of this policy with respect to their own employees.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, hardware, software, operating systems, storage media, network accounts providing electronic mail, Web browsers, and file transfer protocols, are the property of the City and County of San Francisco. These systems are provided for City business purposes only.

3.1 General Use and Ownership

Data created and/or stored on City systems remains the property of the City and County of San Francisco. There is no guarantee of confidentiality of information stored on any network device belonging to the City.

- The City's Employee Handbook clearly states the City's computer networks, computer systems, telephones, cell phones, fax machines and other City property are to be used for City business purposes only. The handbook sections "Use of City and County Property for Business Purposes Only" and "Computers and Data Information Systems" state, in relevant part:
    - Authorized employees or contractors may monitor equipment, systems, and network traffic at any time for security, network maintenance and policy

compliance purposes. Typically, monitoring will be done by departmental IT staff or the Department of Technology.

- The City reserves the right to conduct audits on a periodic basis to ensure compliance with this policy.
- The City reserves the right to forensically or otherwise examine City-owned electronic devices, including but not limited to computer systems, networks, telephone systems and cell phones.

- The complete CCSF Employee Handbook is at www.sfdhr.org/index.aspx?page=30.

3.2 Use of Personally Owned Devices

Employees may use personally-owned devices to access City networks, subject to the following:

3.2.1 Using personally-owned devices to conduct City business

Prior to accessing the City network to conduct City business using a personally owned device, employees must obtain permission from their appointing officers or designees. Access to City networks is limited to City business only, and subject to all City-wide and departmental monitoring systems and policies, including but not limited to the prohibition of discrimination and harassment in the workplace.

The City's networks are City property and therefore fall under the Employee Handbook sections mentioned in section 3.1 of this document.

3.2.2 Using personally-owned devices to conduct personal business

Employees may use their personally owned devices to access City networks designated for public or guest access to conduct personal business during defined rest or meal periods, and subject to any applicable departmental limitations and other City policies, including but not limited to confidentiality, conflict of interest, general conduct, harassment, and discrimination.

3.3 Security and Proprietary/Confidential Information

Information contained on the Internet/Intranet/Extranet-related systems may be proprietary or confidential, as defined by the City or department confidentiality guidelines. An example of proprietary information may be a specific software application. Examples of confidential information may include, but are not limited to: employee medical information, employee personal data, vendor and bidder information, attorney/client correspondence, examination and job application materials, and other data. Employees may or may not have access to

proprietary and/or confidential information, depending on the business need for access to this type of information.

Authorized users are assigned network accounts based on defined business needs. These accounts are called User Level Accounts. Each employee's access to specific types of information is defined in his or her User Level Account. All employees, regardless of level of access, should take all necessary steps to prevent disclosure of any proprietary and/or confidential information to anyone not authorized to access this information.

In the event a City employee receives a request for information, including requests submitted under the Public Records Act and/or Sunshine Ordinance, the employee must work with his or her department's designee to ensure that in fulfilling requests they do not release any proprietary and/or confidential data to the public.

4. Enforcement

Violators of this policy may be subject to appropriate disciplinary action, up to and including termination of employment and/or legal action.

5. Definitions

Terms	Definitions
Employee Handbook	CCSF's Employee Handbook may be found at www.sfgov.org

6. Revision History

Effective Date	Employee Name	Description
TBD	Jeana Pieralde, CISSP	Chief Security Officer