

**Information Security Policy****1.7.6****PURPOSE**

The City's Information Technology and Police Departments are jointly responsible for the physical protection of the City's information technology systems and electronic data. The purpose of this policy is to identify the authorities and protocol for gathering, keeping and reporting on confidential information about the current status of the security of the organization's information technology systems.

**AUTHORITIES**

The Chief Information Officer (CIO) has the duty to administer the City's central computer systems and functions, manage the City's communication services and provide advice and recommendations regarding current and proposed computer system maintenance and planning. The Police Chief has the duty to administer the operation of the Police Department, perform services and functions relating to crime prevention and crime investigation. Together, the CIO and the Police Chief are required to perform such other functions that the City Manager authorizes or requests. The City Manager hereby authorizes them both to be responsible for and to enforce the following policy.

**POLICY**

1. It is the policy of the City of San Jose to ensure the ongoing critical City operations by establishing and maintaining proper Security of its Information Technology Systems and the data contained therein against terrorist, criminal or unauthorized attack or disclosure.
2. The City shall ensure that proper technology, systems and procedures are in place to prevent the potential for such attacks or disclosures.
3. The City shall maintain all information that would make the City vulnerable to such attacks or disclosures in a secure and confidential manner.
4. The City shall from time to time conduct internal and external audits, surveys and tests of its own security procedures and policies.
5. Documents prepared for the City that assess its vulnerability to terrorist attack or other criminal acts intended to disrupt the City's operations including its Information Technology systems for distribution or consideration in a closed session of the City Council shall be kept confidential and secure.
6. Documents gathered for the purpose of assessing the security procedures of the Police Department including City Information Technology systems that the department is responsible for shall be kept confidential and secure.
7. The following precautions should be followed with respect to confidential data subject to this Policy:
  - a) Stored data should be kept in a secure location that is not publicly accessible with access granted on a "need to know" basis as determined by the Chief Information Officer or designee, or the Chief of Police for law enforcement data.

**Information Security Policy****1.7.6**

- b) Data in transit across the City network should be limited on a “need to know” basis as determined by the Chief Information Officer or designee, or the Chief of Police for law enforcement data described under this code.
  - c) Data in transit across public networks (all networks other than the City’s) will be encrypted and distributed limited on a “need to know” basis as determined by the Chief Information Officer or designee, or the Chief of Police for law enforcement data.
8. Data stored on non-City systems or portable devices (such as laptops, CDs, USB memory sticks, etc.) will be encrypted.
9. At the conclusion of security audits, all data (including back-ups) in the possession of non-City parties will be destroyed with certification of such destruction supplied to the City.
10. At the conclusion of security audits, all data generated in support of the project must be destroyed with a sole copy stored in a secure location as designated by the Chief Information Officer.
11. Any agreement entered into by the City in furtherance of the performance of this Policy shall contain provisions requiring adherence to the provisions of this Policy.

/s/ Randall Murphy  
Chief Information Officer

6/23/2008  
Date

/s/ Robert L. Davis  
Chief of Police

6/23/2008  
Date

Approved:

/s/ Christine Shippey  
Assistant City Manager

6/23/2008  
Date