Information and Systems Security Policy 1.7.6

PURPOSE

This policy outlines and establishes the governance and management of information, information systems, standards, guidelines, and procedures required for the City of San José ("City") to:

- Maintain accessible, reliable, and secure information systems;
- Maintain integrity, availability, and confidentiality of information by protecting it from unauthorized disclosure, modification, and destruction;
- Define the objectives and principles for data and systems protection; and
- Define roles and responsibilities for all users of the City's systems, networks, and information assets.

The City's information technology systems and the data contained therein will be built, operated, and maintained utilizing the City's Security Standards Handbook.

SCOPE

This Policy applies to:

1. All City information systems, networks, and information assets (whether located onsite, off-site, or in cloud-based locations); and
2. All users of the City's information systems, networks, and information assets including, but not limited to, employees (full-time, part-time), interns, consultants, contractors, and volunteers.

GENERAL PRINCIPLES

The City's Information and Systems Security program and principles build adherence to a comprehensive security architecture that achieves high defense and resilience, protecting the information, operations, and resources that support City services to the community.

The key objectives of the Information and Systems Security Policy are to:

- Protect City records from unauthorized disclosure, modification, or deletion;
- Maintain processes to assess and manage security risks to City information as new threats emerge and technology and business practices change;
- Support compliance with applicable laws and regulations;
- Prioritize and implement controls to prevent security problems;
- Provide the minimum access to data and systems needed to carry out staff function;
- Allow access to confidential information based on staff function and duties;
- Ensure separation of duties when performing critical transactions; and

- Incorporate security throughout the application lifecycle (design, development, maintenance, and retirement) and network design based on data classification (Public, Sensitive, Confidential).

The guiding principles for the Information and Systems Security Policy include:

- The Security Office is responsible for the operational security of the City information systems, networks, and information assets to ensure the confidentiality, integrity, and availability of these resources.
- Information systems, network, and information assets critical to City operations shall be maintained to prevent terrorist, criminal or unauthorized attack or disclosure.
- The physical security of all data processing assets, network, or security equipment shall be maintained to prevent unauthorized access, tampering, or criminal use.
- No individual should have, or appear to have, conflicting or unsupervised duties that might jeopardize the security of information or information systems. No one individual may approve, and simultaneously execute a sensitive operation.
- Any computing device containing City data shall be disposed/repurposed after all data has been deleted in accordance to the Information Security Standards Handbook.
- Any agreement with the City shall contain provisions requiring adherence to the provisions of this Policy.

RESPONSIBILITIES

- The Chief Information Officer (CIO) is responsible for directing City IT resources, policies, projects, services, and coordinating the same with other City departments. The CIO shall designate the City Information Security Officer (CISO) to actively ensure the security and resilience of the City's information systems and assets.
- The CISO is responsible for overseeing the enterprise security infrastructure, cybersecurity operations, updating security policies, procedures, standards, guidelines, and monitoring policy compliance such as, but not limited to, the California Law Enforcement Telecommunication System (CLETS), Criminal Justice Information Systems (CJIS), Health Information Privacy and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS).
- The CISO or designee shall provide security awareness training to all employees annually, or if appropriate, periodically. At the conclusion of the security awareness training, employees will be asked to acknowledge completion of the training, and agreement to comply with this Policy. This acknowledgement must be retained by the CISO or designee.
- The CISO or designee is responsible for reporting to the CIO any substantive known or perceived information security incidents, breaches or vulnerabilities and is responsible for executing the incident response plan when applicable.
- The CISO or designee shall annually conduct reviews of security procedures and policies, and a citywide security assessment through a qualified third-party security assessor at least bi-annually.

- The CISO or designee is responsible for notifying California residents and the Attorney General of data breaches in accordance to California Civil Code §1798.29 and §1798.82.

POLICY

Requirements for IT/Security contracts

Any Contractor access to City information systems, networks, and information assets must comply with the following:

- The City Information and Systems Security Policy and standards applicable to the service being provided shall be provided to the contractor before access is granted. For CJIS systems, the Police Department (PD) shall require and administer fingerprinting, before access is granted.
- Agreements relating to information technology systems or services should include licensing arrangements, define the ownership of intellectual property rights, and provide for audit rights including, if appropriate, independent audit reports outlining the contractor's security control environments that support the City information assets.
- Security reviews should be performed as part of the purchasing process of any IT system.
- Authorization for contractors with privileged access to City information systems, networks or information assets must expire and require renewal on a periodic basis (annually, or other period as appropriate) and must include PD approval if the privileges include CJIS security boundary.
- Contractor access to City information systems, networks or information systems must be explicitly granted by the City only when it is linked to a specific documented responsibility. Access must be limited to only those information assets required to fulfill the responsibility.
- Upon termination of an agreement, the following actions must be performed in a timely manner as dictated by the terms of the agreement:
    - All information sharing connections and/or mechanisms including network access must be disabled and removed;
    - All contractor's accounts must be disabled and removed; and
    - The City's information assets must be returned in a manner that the City can consume and any information assets used at the contractor's premise must be permanently destroyed by the contractor.

Expectations of Privacy

- Employees shall have no expectation nor right of privacy on any systems or networks provided by the City from their role as an agent. All information, stored and real-time, contained within a system or network is owned by the City, and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized City personnel. The City reserves the right to disclose any potential evidence of crime found on City systems for any reason.

- The City is subject to the California Public Records Act (CPRA). This means that any writing containing information relating to the conduct of the public's business that is prepared, owned, used, or retained by the City, regardless of physical form or characteristics, is a public record. Upon request, the City must disclose a public record unless part or all of the record is protected by an exemption specifically described in the CPRA. Additional information is available in the City's Public Records Policy and Protocol, City Administrative Policy Manual Section 6.1.1.

Policy Enforcement

All employees of the City, whether permanent or temporary, interns, volunteers, contractors, consultants, vendors, and other third parties are required to abide by the Information and Systems Security Policy.

Information Technology Systems and the data contained therein will be built, operated, and maintained utilizing the City's Security Standards document. The City's Security Standards is located on the City Intranet under the Information Technology Department.

All remote access to the City's computing network shall be managed by the Information Technology Department. All requests for and uses of remote access shall conform to the stated procedures for authorization and implementation located on the City Intranet under the Information Technology Department.

VIOLATIONS OF THE INFORMATION AND SYSTEMS SECURITY POLICY

Information and systems security is the responsibility of every employee of the City. Violations of any section of the City Information and Systems Security Policy, including compromise or mishandling of City information, may be subject to disciplinary action, up to an including termination. Infractions that violate local, state, federal or international law may be remanded to the proper authorities.

GLOSSARY

Information Asset– A definable piece of information regardless of format that is recognized as valuable to the organization.

Information System/System– A hardware and/or software solution for collecting, creating, storing, processing, and distributing information, typically including hardware and software.

Integrity– The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

IT Security– Practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Protection of Confidentiality, Integrity, and Availability of data.

Network– A system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables that is used to transmit or receive information.

Security Infrastructure– Any hardware or software solution storing, processing, transmitting, and analyzing security related data exclusive of other functions.

Approved:

/s/ Rob Lloyd
Chief Information Officer

April 19, 2019
Date

Approved for posting:

/s/ Jennifer Schembri
Director of Employee Relations
Director of Human Resources

April 19, 2019
Date