CITY OF
SAN JOSE
CAPITAL OF SILICON VALLEY

City of San José

Information Security Standards Handbook

Version 1.3

December 2021

1 Contents

1 Introduction

This handbook serves as the foundation on which the City of San José are to develop, build, implement, and operate information systems. The handbook provides guidance implementing the requirements of CSJ networks and systems.

The scope and contents of this handbook will be updated as new capabilities are added to CSJ systems, as security policies are updated, and as both user experiences and user needs change.

This handbook addresses only information security and is issued as implementation guidance under the authority of the CSJ Chief Information Officer (CIO) through the City Information Security Officer (CISO).

The aspects of information security covered by this Handbook are comprehensive, they pertain to personnel, physical, information, investigations, emergency preparedness.

2 Authorities

- City of San José, “Information and Systems Security Policy” 1.7.6, April 19, 2019.
- NIST Special Publications (SP) 800-53, Rev 4, “Security and Privacy Controls for Federal Information Systems and Organizations” April 2013 with updates as of January 15, 2014.
- NIST Special Publications (SP) 800-92, “Guide to Computer Security Log Management” Sept 2006.
- NIST Cybersecurity Framework (CSF) Version 1.1, Published on April 16, 2018.
- Payment Card Industry Data Security Standard (PCI DSS) Version 3.2.1, Published by PCI Security Standards Council June 2018.
- Criminal Justice Information System (CJIS) Security Policy (CSP) Version 5.7, Published by Federal Bureau of Investigation.
- California Business and Professions Code
- Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003.

3 Roles and Responsibilities

- CIO – Ensure security of information systems
- CISO – Define and implement security program
- Cybersecurity Office – Ensure operational security
- Application Team – Secure application systems
- Desktop Support Team – Secure end user systems
- Network Team – Secure infrastructure
- Server Team – Secure systems and platforms

4 Security Objectives

- 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;
- Incorporate security throughout the system development lifecycle (design, development, maintenance, and retirement); and
- Design systems to protect data based on classification (Public, Sensitive, Confidential)

5 Security Guiding Principles

- 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.
- Documents including security procedures prepared for the City that assess its vulnerability to attack or other criminal acts intended to disrupt City operations including its information or technology systems shall be treated as confidential and secure.
- 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 or designee. Third parties must provide certification of such destruction.
- Any agreement with the City shall contain provisions requiring adherence to the provisions of this Policy.
- New systems shall be architected utilizing a three-tier reference architecture that separates Internet exposed systems from the internal network via a De-Militarized Zone (DMZ) tier and further separates sensitive data (i.e. databases) via a data tier.

6 The Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

6.1 Methodology

The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. An example of Framework outcome language is, "physical devices and systems within the organization are inventoried."

The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories for each Function, and matches them with example Informative References, such as existing standards, guidelines, and practices for each Subcategory.

6.2 Current Profile

A Framework Profile ("Profile") represents the cybersecurity outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important. They can also add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

6.3 Control List

The list of selected controls included in the security baseline can be found as Appendix A: List of Controls. The list of selected controls and their mappings to other security frameworks is maintained as a separate document.

7 Management Controls

This section specifies the security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

7.1 Contractors and Outsourced Operations / Acquisitions

Purpose - The City of San José relies heavily upon third parties to provide critical services, resources, and assets, the unavailability of which may represent a significant risk to the information system. Securing the supply chain from disruption is accomplished by risk assessments, vendor contracts, and ensuring asset availability. This standard for outsourced operations shall ensure that one (1) or more of the following: Memorandum Of Understanding (MOU), Memorandum Of Agreement (MOA), Service Level Agreement (SLA), are established in accordance with all legal requirements of the City Attorney Office, with external third parties to ensure the availability of critical services and resources.

Scope – Any service or resource that cannot be provided internally by the City of San José falls under the scope of supply chain protection. Guaranteeing availability of resources is just as important as providing availability of systems and networks.

Impact – The lack of needed resources may impact the availability of the information system if needed components, personnel, or services are not present. The City of San José relies upon these external third party resources which can only be guaranteed through contracts and agreements (MOU, MOA, SLA, etc.). Important components may include: laptops for new users, parts to maintain critical servers, even power cords and display adapters. Important personnel may include contractors, consultants, and third party vendors providing specialized knowledge. Critical services may include Internet connectivity or vendor services like office applications and training materials.

7.1.1 Internet Availability

Outsourced cloud services and third party interconnections require always-on, high-bandwidth, dedicated connection(s) to the Internet. Resources provided by an external Internet Service Provider (ISP) are necessary to facilitate Internet connectivity.

- The City of San José shall maintain one of MOU, MOA, SLA with an ISP to provide Internet connectivity in support of mission/business processes.
- The City of San José shall maintain a network architecture that supports Internet connectivity availability requirements to enable critical mission/business processes.

7.1.2 Device Default Configuration

Information security components shall be purged of default vendor configurations, accounts, and passwords subsequent to acquisition and re-implemented with a standard baseline configuration prior to deployment.

7.2 Program Management

Purpose – The City of San José must ensure that it has a program to operate information systems in a secure and consistent manner, maintaining the confidentiality, integrity, and availability in compliance with all applicable regulations. This Program Management Standard defines the structure, approach, and requirements which shall be documented and maintained in the Information Security Program Plan.

Scope – The Information Security Program Plan reflects information security guidance at the highest level, applicable to every part of the City of San José. It is a collection of standards, programs, strategies, plans, and procedures which collectively outline the implementation of all aspects of a secure information system. The Program Management Standard primarily assigns management responsibility for implementing key sections of the Information Security Program Plan.

Impact – A security program provides the framework for maintaining the desired security level by assessing risks, deciding how to mitigate them, and planning for how to keep the program and security practices up to date. Without a well-defined security program, all aspects of data and systems protection are more difficult and less mature. A holistic risk-based approach ensures the alignment of information security management and protection goals with business processes.

7.2.1 Senior Information Security Official

The City of San José shall appoint a City Information Security Officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. This process is an integral part of the Information Security Program Plan.

7.2.2 Information Security Resources

The City of San José shall ensure that all capital planning and investment requests include the resources needed to implement the information security program. This process is an integral part of the Information Security Program Plan.

7.2.3 Plan of Action and Milestones (POA&M) Process

The City of San José shall ensure that all deviations and deficiencies from the Information Security Program Plan are captured and documented within a Plan of Action and Milestones. This process is an integral part of the Information Security Program Plan.

7.2.4 Information System Inventory

The City of San José shall ensure that all components of the information system (including: physical assets, virtual systems, applications, and sensitive data) are captured in an inventory as specified further in this standards document. This process is an integral part of the Information Security Program Plan.

7.2.5 Information Security Measures of Performance

The City of San José shall develop, monitor, and report measures of performance which are outcome-based metrics used to measure the effectiveness and/or efficiency of the information security program and the security controls employed in support of the program. This process is an integral part of the Information Security Program Plan.

7.2.6 Enterprise Architecture

The City of San José shall develop an enterprise architecture with consideration for information security and the resulting risk to City operational environments, City assets, and individual users of City information systems, networks, and information assets. The Enterprise Architecture shall describe the overall philosophy, requirements, and approach to be taken regarding the design of a secure architecture. This process is an integral part of the Information Security Program Plan.

7.2.7 Critical Infrastructure Plan

The City of San José shall identify all information system components, assets, networks, services, business processes, and physical infrastructure which are considered critical to continued operations and implement protection strategies based on the prioritization of criticality. This process is an integral part of the Information Security Program Plan.

7.2.8 Risk Management Strategy

An effective strategy for maintaining information security is achieved by taking a risk-based approach; risk is identified and managed based on: threat level, impact, risk appetite, program maturity, capability, gap analysis, and regulatory requirements. The City of San José shall develop, implement, and maintain a comprehensive strategy to manage risk to organizational operations and assets associated with the operation and use of information systems. The Risk Management Strategy shall detail a foundational risk management framework, and specify a risk assessment process that Is performed at least annually and upon significant changes to the environment. The City shall take a risk-based approach to continually refining and improving the security of its overall information system. This process is an integral part of the Information Security Program Plan.

7.2.9 Security Authorization Process

The City of San José shall define a process by which it can determine the security state of information systems and environments (Continuous Monitoring), identify the risk associated with allowing the system to operate (Risk Management), and ensure identification and mitigation/acceptance of deficiencies (Plan of Action and Milestones) prior to allowing production operation to commence. This process is an integral part of the Information Security Program Plan.

7.2.10 Business Process Definition

The City of San José shall define mission/business processes with consideration for information security and the resulting risk to City operational environments, City assets, and individual users of City information systems, networks, and information assets.

By identifying the City's individual mission/business processes, a determination can be made regarding the information protection needs. Information protection needs determine the required security controls applied to the associated information systems. Inherent in defining the information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. This process is an integral part of the Information Security Program Plan.

7.2.11 Information Security Workforce

The City of San José must ensure that it has an information security workforce program sufficient to institutionalize core information security capabilities and retain qualified personnel needed to protect organizational operations, assets, and individuals. The program may include development and improvement of the information security workforce through:

- Defining the knowledge and skill levels needed to perform information security duties and tasks.
- Developing role-based training programs for individuals assigned information security roles and responsibilities.
- Providing standards for measuring and building individual qualifications for incumbents and applicants for information security-related positions.
- Recommending information security career paths to encourage information security professionals to advance in the field and fill positions with greater responsibility.
- Enabling the City to fill information security-related positions with qualified personnel.

This process is an integral part of the Information Security Program Plan.

7.2.12 Continuous Monitoring

The City of San José shall develop, implement, and maintain a continuous monitoring strategy, which establishes requirements for ongoing security control assessments, network monitoring, data flow monitoring, vulnerability scanning, and penetration testing. The Continuous Monitoring Strategy identifies the monitoring objectives, which determine the selection of controls to facilitate the extent and frequency of monitoring. The Continuous Monitoring Strategy also identifies the reporting and alerting objectives to inform environmental awareness and incident response capability. This process is an integral part of the Information Security Program Plan.

7.2.13 Threat Awareness Program

The City of San José shall maintain a threat awareness program that serves to keep the Cybersecurity Office informed of current threats and inform the incident response capability. The program may include but not limited to:

- Insider threats and Advanced Persistent Threats (APT)s
- Cross-organization information-sharing (i.e., tactics, techniques, and procedures)
- Threat intelligence (i.e. Indicators of Compromise (IoC)s)

This process is an integral part of the Information Security Program Plan.

7.2.14 System Boundary

The City of San José shall define an explicit authorization boundary for the information system, which contains all information system components. The boundary represents a point of demarcation where components inside fall within the scope of the Information Security Program Plan. All City owned assets must fall within the boundary of an authorized security plan. This process is an integral part of the Information Security Program Plan.

7.2.15 Credit Card System and Information Protection

The City of San José has a critical business need to receive credit card payments in exchange for services and goods. Part of handling Cardholder Data (CHD) is complying with regulations mandating the secure storage and transmission of such data. The Payment Card Industry Data Security Standard (PCI DSS) provides a detailed structure for securing CHD. Many of these requirements provide synergy with the information security goals identified by the City, and as such shall be integrated with the Information Security Program Plan and the Information Security Standards presented in this document. The Credit Card System and Information Protection Standard shall provide several requirements in support of the PCI DSS.

Cardholder Data (CHD) includes any of the following:

- the full contents of any track (from the magnetic stripe located on the back of a card)
- equivalent data contained on a chip
- The cardholder’s name (only sensitive if combined with other CHD)
- Primary Account Number (PAN)
- Expiration date
- Service code
- card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions)
- personal identification number (PIN) or the encrypted PIN block

The following Credit card handling requirements shall be adopted:

7.2.15.1 CardHolder Data Storage

Per PCI DSS 3.1 & 3.2 CHD storage amount and retention time shall be minimized to that which is required for legal, regulatory, and/or business requirements.

- CHD shall be securely deleted when no longer needed.
- A quarterly review shall identify and securely delete stored CHD that exceeds defined retention.

- Sensitive authentication data is not stored after authorization (even if encrypted). If sensitive authentication data is received, all data is rendered unrecoverable upon completion of the authorization process.
- PAN is rendered unreadable anywhere it is stored (including on portable digital media, backup media, and in logs).
- Card verification code or value shall never be stored after authorization.
- Personal identification number (PIN) or encrypted PIN block shall never be stored after authorization.

7.2.15.2 CardHolder Data Restrictions

Per PCI DSS 3.3 & 3.4

- Access to CHD shall be restricted to users with business justification for such access.
- Mask PAN when displayed; the first six or last four digits are the maximum number of digits to be displayed without business justification.
- Strong encryption per standards section 9.6 shall be used anytime CHD is stored.

7.2.15.3 CardHolder Data System Firewall

Per PCI DSS 1.4 portable devices connecting to the CHD environment shall have firewall software installed, configured, and running.

7.2.15.4 CardHolder Data Encryption

Per PCI DSS 3.4.1 CHD shall not be encrypted based upon integrated Operating System disk-level encryption that utilizes native credentials for authentication and access control.

- CHD shall always be encrypted when at-rest and in-transit.

7.2.15.5 CardHolder Data Key Management

Per PCI DSS 3.6 sound key management principles are in use.

7.2.15.6 CardHolder Data Lockout Requirements

Per PCI DSS 8.1.7 user account lockout shall remain locked for a minimum of thirty (30) minutes or until a system administrator resets the account.

7.2.15.7 CardHolder Data Credential Requirements

Per PCI DSS 8.2.4 passwords/passphrases shall be changed at least once every ninety (90) days.

7.2.15.8 CardHolder Data Account Requirements

Per PCI DSS 8.5:

- Generic user IDs are disabled or removed.
- Shared user IDs do not exist for system administration and other critical functions.
- Shared and generic user IDs are not used to administer any system components.

7.2.15.9 CardHolder Data Database Access

Per PCI DSS 8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

- All user access to, user queries of, and user actions on databases are through programmatic methods.
- Only database administrators have the ability to directly access or query databases.
- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

7.2.15.10 CardHolder Data Tampering Detection

Per PCI DSS 9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

- Maintain accurate list of physical devices.
- Periodically inspecting devices to look for tampering or substitution.
- Training personnel to be aware of suspicious behavior and to report tampering or substitution of devices.

7.2.15.11 CardHolder Data Log Review

Per PCI DSS 10.6 Perform daily log review of the following:

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD
- Logs of all critical system components
- Logs from firewalls, IDS, authentication servers, e-commerce servers, malware detection

Per PCI DSS 12.10.5 Create security incidents upon discovery of anomalies due to log reviews.

7.2.15.12 CardHolder Data Log Retention

Per PCI DSS 10.7 configure log storage to retain at least one (1) year of historical log data, with at least three (3) months immediately available for analysis (e.g. online, archived, or restorable from backup).

7.2.15.13 CardHolder Data Intrusion Detection

Per PCI DSS 11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.

Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

7.2.15.14 CardHolder Data File Integrity Monitoring

Per PCI DSS 11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

7.3 Privacy

The need to protect an individual's privacy is as important today as it was in 1974 when the Privacy Act first sought to balance the government's need to collect information from an individual with a citizen's right to be notified as to how that information was being used, collected, maintained, and disposed of after the requisite period of use. Privacy, with respect to Personally Identifiable Information (PII), is a core value that can be obtained only with appropriate legislation, policies, procedures, and associated controls to ensure compliance with requirements. Privacy also involves each individual's right to decide when and whether to share personal information, how much information to share, and the particular circumstances under which that information can be shared. Organizations cannot have effective privacy without a basic foundation of information security. The City of San José shall implement this Privacy Standard, in conjunction with the Privacy Policy developed under the guidance of a City privacy official.

Documentation of Information Collected

The Data Inventory Standard referenced in section 8.1.6 shall support the identification of all collected PII, including if it is shared and with whom.

Privacy Impact Assessment (PIA)

The City of San José shall conduct a Privacy Impact Assessment (PIA) for information systems, programs, or other activities that pose a privacy risk in accordance with the Privacy Policy.

Minimization of Personally Identifiable Information (PII)

The City of San José shall collect and store the minimum amount of PII that is necessary to conduct business processes and operations. PII shall be removed when the data is no longer required for business purposes in accordance with the public records retention policy and the Media Sanitization Standards set forth in section 8.6.4. The City of San José shall, where appropriate, use anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

Data Integrity

The City of San José shall take reasonable steps to confirm the accuracy and relevance of PII

7.4 Recovery Planning

Purpose – The City of San José depends on critical information systems and technologies to process and manage data, transactions, audits, and reporting to deliver uninterrupted services on behalf of internal employees and the general public. The Recovery Planning Standard defines the recovery requirements, parameters, and criteria to accomplish three key objectives:

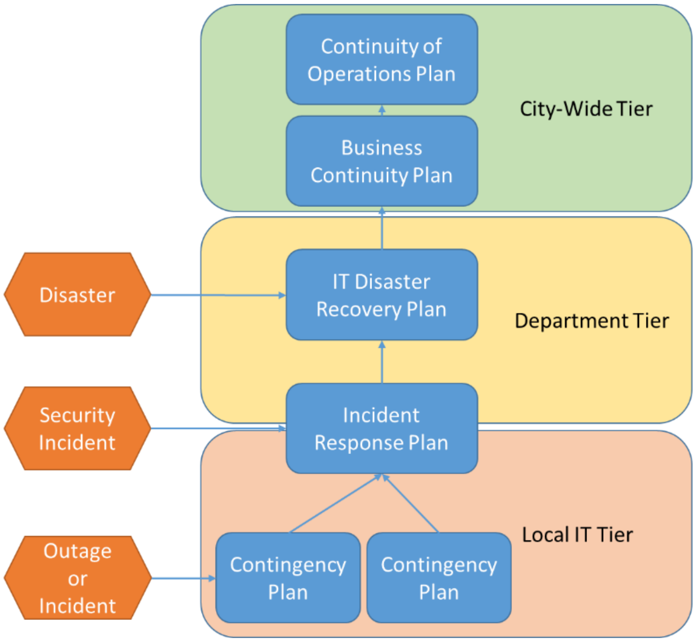
- Mitigate risk exposures related to outages, incidents, and disasters
- Maintain continuity of critical processes and services to support recovery of information systems and technology capabilities
- Recover information systems and technologies based on the requirements in order to meet the expectations of City of San José business groups, while maintaining a cost effective level of disaster recovery capability by City of San José Information Technology (IT)

Scope – This standard is applicable to all users of City of San José information systems, networks and information assets managed by ITD, including but not limited to full-time regular employees, part-time regular employees, temporary employees, consultants, contractors, and volunteers.

This standard addresses continuity and recovery requirements to appropriately mitigate and manage risks from interruptions of IT services due to outages, incidents, and disasters across all City of San José locations where ITD provides infrastructure and services.

Recovery Strategy

The City of San José shall take a tiered approach to ensure the capability to resume business operations after disruption due to outages, incidents, and disasters.



- An incident with city-wide impact to business operations will trigger the Business Continuity Plan (BCP) and/or Continuity of Operations Plan (COOP). These high-level plans may incorporate or activate lower level plans due to the severity and broad impact of the incident (e.g. a major flood disrupts city-wide operations and a disaster is also declared, activating the DRP).
- A large-scale or wide-impacting event may be deemed a disaster, triggering activation of the Disaster Recovery Plan (DRP). The DRP will refer to lower level plans during the recovery and reconstitution phase (e.g. need to redeploy servers damaged by fire using the CP unique to that system).
- When an incident is deemed to be a security incident, the Incident Response Plan (IRP) will be activated. Unique phases to the IRP include containment and eradication of threats. The IRP could be used for security incidents with either a localized impact (only one or two CPs are needed to recover) or a wider impact (where the DRP and/or BCP might also be activated).
- The Contingency Plan (CP) is a technical, low level plan that has a very narrow scope. Procedures outlined in this plan may be coordinated as part of a larger effort due to activation of higher level plans. The CP provides unique system specific procedures to return a system to operational status quickly.

Computing Environment

- IT shall implement and maintain high-availability architectures and redundant services eliminating Single Points of Failure (SPOF), where possible, in support of the business criticality and RTO for systems in the environment.
- IT shall ensure the required RTO and RPO for data recovery and data loss is met.
- IT shall use the following application tiering structure to define RTOs and Service Delivery agreements:

Tier	Availability Prod DC/DR DC	Fail-Over Type and Definition	RTO	RPO
0	Active/Active	Automatic, Always on	Seconds	No Data Loss
1	Active/Passive	Manual intervention - Trigger on	Minutes	<15 min
2	Active/Warm	Manual preparations	Hours	<24 hours
3	Active/Pre-Provisioned Cold	Manual builds & data restores	Hours & Days	Disk Back-up
4	Active/Cold	Manual purchases/builds & Data restores	Days	Tape Back-up

Data Stores and Databases

- IT shall use the following data store and database tiering structure to define RTOs and RPOs for Service Delivery agreements:

Tier	Availability Prod DC/DR DC	Data Fail-Over Type and Definition	RTO	RPO
0	Active/Active	Transaction Based Replication, Distributed DB, Bi-Directional Replication Data	Seconds	No Data Loss
1	Active/Available	Block Level Replication, Transaction Based Replication, Incremental Backups, Uni-Directional Replication Data	Minutes	<15 min
2	Active/Warm	Uni-Directional Replication or Replicated Backup	Hours	<24 hours
3	Active/Pre-Provisioned Cold	Disk Back-up	Hours & Days	Hours to Days
4	Active/Cold	Disk/Tape Back-up	Days	Days

7.4.1 Business Continuity Program

- A Business Continuity Plan (BCP) shall be developed, documented and maintained for City of San José business departments that have viable, manual or work-around capabilities identified to support critical process continuity and service Recovery Timeframe Objectives (RTOs)
- BCP components shall include the following content, and support CSJ Continuity of Operations Plan (COOP)
    - Risks, requirements and SLA's, as defined by the BIA (min. <3 years) to support ITD RTO's
    - Governance structure including roles and responsibilities
    - Management
    - Technologies
    - Facilities
    - Operations
- City of San José employees and Contractors shall be provided appropriate training and made aware of BCP responsibilities to respond upon activation of the BCP.
- BCPs shall be reviewed, revised and tested at least annually.

7.4.2 Disaster Recovery Program

An IT Disaster Recovery Plan (DRP) shall be developed, documented and maintained for the City of San José that denotes IT Service restoration capabilities, solutions, and actions to support critical process continuity.

- DR Plan components shall include the following content, and support the City of San José's current Continuity of Operations Plan (COOP) as appropriate
    - Governance structure including roles and responsibilities
    - Management
    - DR Planning Strategy
    - Recovery Procedures
    - Activation Criteria
- IT shall be made aware of and involved in plans, designs, decisions, and engineering related to the integration of IT Services for which IT will have ownership or management in any way, as the business departments begin to champion or consider initiatives for IT Service change, improvement, or availability.
- City of San José employees and Contractors shall be provided appropriate training and made aware of DRP responsibilities to respond in a declared disaster.
- DRPs shall be reviewed, revised and tested at least annually.

7.4.3 Contingency Planning

The City of San José shall ensure a Contingency Plan exists for each logical group within the information system, which includes detailed procedures to recover systems and services, and to verify full functionality. Contingency Plans shall be reviewed, revised and tested at least annually.

- IT shall ensure the required RTO and RPO for data recovery and data loss is defined.
- IT shall conduct annual DR Database (DB) and data fail-over and restoration testing for all critical data stores validating RTOs, DR recovery capability and data integrity.

7.4.4 Alternate Site

- If a secondary DR DC is established it shall be at an appropriate distance from the Production DC (generally no less than 300-500 miles), Tier 3+ and shall avoid proximity to high-risk threats (i.e. airports, same earthquake zones, etc.)
- If a secondary DR DC is established it shall align to Business capabilities expansion objectives and direction.
- IT shall ensure that data backups are maintained at an offsite location, at an appropriate distance from the primary site.

7.5 System Development Life Cycle (SDLC)

Purpose – Consideration of security in the System Development Life Cycle (SDLC) is essential to implementing and integrating a comprehensive strategy for managing risk for all information technology assets in an organization. The City of San José shall ensure a secure process to address security throughout all stages of the SDLC regardless of project management methodology. This SDLC Standard shall provide requirements for ensuring security principles and best practices throughout the entire SDLC process.

Scope – The approach for ensuring security and managing risk specified in this SDLC Standard shall apply to all projects with an information technology component regardless of department responsible for the system or the underlying project management approach employed.

Impact - Organizations may realize the value of integrating security into an established SDLC in many ways, including:

- Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation.
- Awareness of potential engineering challenges caused by mandatory security controls.
- Identification of shared security services and reuse of security strategies and tools to reduce cost and schedule while improving security posture through proven methods and techniques.
- Facilitation of informed executive decision making through comprehensive risk management in a timely manner.
- Documentation of important security decisions made during development, ensuring management that security was fully considered during all phases.

- Well-designed solutions promote adoption by end users, as well as confidence to promote continued investment.
- Improved systems interoperability and integration that would otherwise be hampered by securing systems independently.

7.5.1 Agile and Lean processes

The City of San José has chosen to take an Agile approach to project management within the Information Technology Department. As such, the unique security implications must be considered throughout the process.

Secure Scrum

The heart of Secure Scrum is the use of S-Tag and S-Mark. Security-relevant user stories are ranked by their risk and marked in the Product Backlog. The marker is called S-Mark, which can be a sticker, a dot or a color background.

Based on marked user stories, a list of S-Tags is created. An S-Tag describes a security concern. An S-Tag might affect one or many Product Backlog Items. In order words, several Product Backlog items might share the same security concern.

Because Product Backlog Items can change over time to adapt the development process, S-tags can be modified when refining Product Backlog or planning new Sprint. So long as the user story is marked with an S-Mark, the S-Tag must be handled.

The Definition of Done component ensures that the verification of security has been completed to the satisfaction of the security team.

Iteration 0: Environment Set-Up

Most projects will start with an "Iteration 0," when necessary infrastructure is established before delivering features. Pre-production environments provide an entry point into more valuable targets, which is why teams must incorporate greater security measures, especially at this point in the process.

Story Lifecycle

User stories are the base of any agile workflow. Usually at the beginning of a project, the team agrees how these stories are going to move along the wall. This activity should also contain security criteria that stories must meet so they can be considered complete. This is where the decision is made to implement enhancements supporting Secure Scrum.

In Testing

The Quality Assurance (QA) process is a good point in the process to validate security requirements. Specifically, the team's QA process can incorporate checking against attack trees, Cross Functional Requirements (CFRs), and identified security acceptance criteria.

Continuous Improvement

As with any agile process, teams can learn and improve in an iterative manner. Specifically, teams should continuously update their threat model and attack trees as knowledge grows about the product, the systems that are being built, and the interaction between the users and these systems. Continuous collaboration with the security team should occur throughout the development process, not just after implementing a feature or before releasing to production.

7.5.2 Initiation

Key security activities for this phase include an initial project review to determine the following:

- The review evaluates concept of operations; verifies that the concept is viable, complete, achievable, and in line with organizational mission objectives and budgetary constraints.
- The review evaluates performance; ensures that the initial system design has addressed all relevant security requirements.
- The review ensures Enterprise Architecture (EA) alignment with IT vision, standards, and business requirements, as well as alignment with security policy and standards.
- The review evaluates finance; verifies that the system will balance the cost implications associated with implementation versus security controls.
- The review includes an initial assessment of risk to reduce ambiguity in managing overall project risk.

7.5.3 Acquisition & Development

Key security activities for this phase include a mid-project status review to determine the following:

- The review evaluates design; the planned system design and potential integration with other systems as well as incorporation of shared services and common security controls, such as authentication, disaster recovery, intrusion detection, or incident reporting.
- The review evaluates performance; whether the system is delivering, or capable of delivering, to the documented expectation of the owner and whether the system behaves in a predictable manner if it is subjected to improper use. (For example, the ability of the system to maintain availability and data integrity at the expected extreme resource loads.)
- The review evaluates functionality; ensures functional requirements identified are sufficiently detailed and are testable.
- The review detects any major shifts in planned level of effort to ensure cost-benefit ratios are monitored and effective decisions are continued.
- The review may revisit risk management decisions if, the system and/or its security controls and/or its requirements change.

7.5.4 Implementation & Assessment

Key security activities for this phase include:

- Integrate the information system into its environment including applicable security controls.
- Plan and conduct testing of security controls to ensure functionality.
- Authorize the system.

7.5.5 Operation & Maintenance

Key security activities for this phase include:

- Conduct an operational readiness review.
- Manage the configuration of the system.
- Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls.

7.5.6 Decommissioning

Key security activities for this phase include:

- Build and Execute a Disposal/Transition Plan.
- Archive of critical information.
- Sanitization of media.
- Disposal of hardware and software.

7.6 Configuration Management

Purpose – The City of San José would like to maintain consistency within its information system to ease manageability and maximize availability of services. To accomplish this, the City shall ensure that modifications to its information system occur in a controlled and non-disruptive manner. The City must also abide by applicable regulations regarding configuration management. This standard is adopted to promote better communication and participation across City departments.

Scope – Any change with significant impact to the confidentiality, integrity, or availability of a production component of the information system shall be subject to review and approval by a change control body.

Impact – Users with elevated privileges may be able to change important settings without considering the implications or solely for investigative troubleshooting. Certain changes could alter the security posture of the overall information system such that a breach or compromise becomes easier to accomplish and more likely to occur. Without coordination between stakeholders, outages or service disruptions could have a larger impact than expected.

7.6.1 Baseline Configuration

The City of San José shall ensure that all production components of the information system have an associated baseline configuration.

Baselines shall be reviewed at least annually.

Per PCI DSS 1.1.7 firewall and router rule sets shall be reviewed at least every 6 (six) months.

User System Baseline

The baseline configuration shall specify (at a minimum), detailed configuration settings for each of the technical controls specified in section 9 of this standards document.

Server Baseline

The baseline configuration shall specify (at a minimum), detailed configuration settings for each of the technical controls specified in section 9 of this standards document.

Network Device Baseline
The baseline configuration shall specify (at a minimum), detailed configuration settings for each of the technical controls specified in section 9 of this standards document.

7.6.2 Change Management

The City of San José shall ensure that all changes to a production component of the information system potentially impacting confidentiality, integrity, or availability are approved by a change management board prior to implementation.

Per PCI DSS 1.1.1 all changes potentially impacting the secure network must be approved and recorded prior to implementation.

Change Control Board (CCB)
To facilitate controlled change management processes and procedures with an enterprise-wide scope, the CCB shall ensure that proposed changes are documented, reviewed, and applied.

Change Advisory Board (CAB)
To facilitate controlled change management processes and procedures with a departmental or limited scope, the CAB shall review and document proposed changes.

The CAB is a team of people made up of IT management and subject matter experts. The Change Manager chairs the board. The mission of the CAB is to plan and monitor the changes introduced into the IT environment.

Board Responsibilities

- Assesses Business reason and Business Impact.
- Ensures someone has been identified who is accountable for the change.
- Available Change Plan and Recovery Plan exist.
- Assesses technical impact and approves changes to the production environment.
- Reviews the status of a change throughout the change process.
- Determines how to correct any identified problems.
- A post installation review of the completed change to ensure proper and successful implementation.

Impact Analysis
All change requests shall include a statement of impact to the overall system. At least one member of the Cybersecurity Office should participate in change management proceedings to gauge the security impact of proposed changes. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required.

7.6.3 *Change Classification*

The City of San José shall ensure that all changes to the information system are classified according to one the defined types. There are different types of change requests, or change classes, that are typically managed in different ways:

Standard changes are changes to a service or to the IT infrastructure where the implementation process and the risks are known upfront. These changes are managed per policies that the IT organization already has in place. Since these changes are subject to established policies and procedures, they are the easiest to prioritize and implement, and often don't require approval from a risk management perspective.

Normal changes are those that must go through the change process before being approved and implemented. If they are determined to be high-risk, a change board must decide whether they will be implemented.

Emergency changes arise when an unexpected error or threat occurs, such as when a flaw in the infrastructure related to services must be addressed immediately. A security threat is another example of an emergency situation that requires changes to be made immediately.

7.6.4 *Inventory*

The City of San José shall ensure that all hardware and software assets are included as part of a comprehensive inventory.

Physical Asset Inventory
All City resources and assets associated with the information system shall be accounted for in a centralized repository to provide accountability, assist with audit activities, and enable identification of unauthorized devices.

Software Inventory
An accurate and comprehensive list of software installed on each City computing asset shall be maintained in a centralized repository to assist with licensing compliance and enable identification of potentially malicious software.

7.7 Security Assessment and Authorization

Purpose – To provide effective protection of its information system and information system assets (data), the City of San José must continuously monitor, evaluate, and improve the overall security posture of the information system. The purpose of this standard is to provide requirements (guided by the Continuous Monitoring Plan), for performing the following:

- Controls Assessment
- Interconnection Agreements
- Network Monitoring
- Vulnerability Scanning
- Penetration Testing

Identification of security posture is accomplished in part by monitoring, which includes the observation of events occurring:

- at the information system boundary (i.e., part of perimeter defense and boundary protection),

- internally within the information system, and
- from outside the boundary of the information system.

Scope – This standard applies to all City of San José information systems, networks, and information assets including any devices that are interconnected with City owned resources or devices that contain City owned data.

7.7.1 Security Controls Assessment

The City of San José shall ensure that the information system has a comprehensive assessment to determine the effectiveness of security controls at least annually. A testing plan shall be maintained which specifies methods of inspection, responsible individual, and results.

7.7.2 Information Exchange Agreements

Authorizes connections from the information system to other information systems by Information Exchange Agreements.

Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.

Reviews and updates Information Exchange Agreements at least annually, or as needed due to information system changes.

7.7.3 Network Monitoring

Monitors the network as appropriate to: ensure nominal operations, detect security incidents, and correlate other threat intelligence.

7.7.4 Vulnerability Scanning

Performs vulnerability scans of every information system component within the authorization boundary at least on a quarterly basis.

7.7.4.1 Internal Scanning

Performs internal scans originating from within the information system authorization boundary and contain credentials to obtain in-depth results.

7.7.4.2 External Scanning

Performs external scans originating from outside the authorization boundary to obtain an overview of the exposure surface.

7.7.4.3 Ad-Hoc Scanning

Performs ad-hoc scans targeting individual information system components, often specific network ports and services, as necessary to verify integrity and/or correlate other threat intelligence.

7.7.5 Penetration Testing

Performs periodic penetration tests of the information system to identify areas of vulnerability and to test the operational incident response capability.

Per PCI DSS 11.3 A penetration test is performed at least annually or due to change within the environment from inside and outside the PCI boundary to validate proper segmentation, identify exploitable vulnerabilities, and identify application vulnerabilities.

8 Operational Controls

This section specifies the security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

8.1 Data Protection

Purpose – Unauthorized access, disclosure, or destruction of City of San José information assets (data) represents a significant risk and must be protected accordingly. The purpose of this standard is to provide information security requirements for classification and handling of City of San José information assets (data).

Scope – This standard applies to City of San José information systems, networks, information assets, and personnel (including but not limited to full-time regular employees, part-time regular employees, temporary employees, consultants, contractors, and volunteers).

This standard applies to all City of San José information assets (data) stored on city-owned, city-leased, and otherwise city-provided systems and media, regardless of location.

8.1.2 Data Classification

Information assets (data) residing on City of San José information systems and networks shall be classified into one of the following categories: Public, Sensitive, or Confidential. All information assets (data) shall be continuously re-evaluated for potential re-classification.

Public:

Public information assets (data) are non-sensitive information appropriate for external release. This information may be open to the general public and is information with no existing local, national, or international legal restrictions on access or usage. Public information is available to City of San José employees and all individuals or external entities. Public information may be subject to California Public Records Act (CPRA) or Freedom of Information Act (FoIA) unless exempt from disclosure by law.

Information released as Public data shall not violate any pre-existing, signed non-disclosure agreements.

Sensitive:

Sensitive information assets (data) are sensitive if shared outside the City of San José. This information must be guarded due to proprietary, ethical, or privacy considerations and shall be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Sensitive data is generally available to employees and approved non-employees.

Confidential:

Confidential information assets (data) are information that is sensitive within the City of San José and is intended for business use only by specific groups of employees. Confidential information includes but is not limited to: Personally Identifiable Information (PII), Personal Health Information (PHI), Criminal Justice Information (CJI), Cardholder Data (CHD), security documentation (network drawings, IP Addresses, audit findings, passwords, etc.). This information may be protected by statutes, regulations, City of San José policies or contractual agreement. By definition, this information is sensitive in nature and access is restricted. Disclosure is limited to individuals on a "need-to-know" basis. Disclosure to parties outside of the City of San José shall be authorized by the Chief Information Officer or designee, or the Chief of Police, or covered by a binding confidentiality agreement.

8.1.3 Data Storage

The following guidelines apply to storage requirements for different classifications of City of San José information assets:

Public:

- Public information assets (data) has no specific storage requirements.

Sensitive:

- Sensitive information assets (data) shall be stored with an appropriate backup schedule as defined by the owner of the information assets.
- Sensitive information assets (data) shall be stored only on systems owned, managed, or under the control of the City of San José.

Confidential:

- Confidential information assets (data) shall be stored with an appropriate backup schedule as defined by the owner of the information assets.
- Confidential information assets (data) shall be stored only on systems owned, managed, or under the control of the City of San José and that have been designated to contain confidential data.
- Confidential information assets (data) shall be encrypted whenever it is stored (at-rest).

8.1.4 Data Transmission

The following guidelines apply to the transmission requirements for the different classifications of City of San José data assets:

Public

- Public information assets (data) have no specific transmission requirements.

Sensitive

- Sensitive information assets (data) shall only be transmitted to a City of San José owned, managed, or controlled information system.
- Sensitive information assets (data) shall only be transmitted to authorized information systems outside of the City network for City of San José official business purposes only.

Confidential

- Confidential information assets (data) shall only be transmitted to a City of San José owned, managed, or controlled information system that has been designated to contain confidential data.
- Confidential information assets (data) shall only be transmitted to authorized information systems outside of the City network with prior authorization from the Chief Information Officer or designee, or the Chief of Police per City Administrative Policy Manual section 1.7.6.
- Confidential information assets (data) shall be encrypted (using encryption mechanisms approved by the Cryptography standards set forth in section 9.6) when the data is transmitted (in-transit).

8.1.5 Data Destruction

The following guidelines apply to the destruction of data for the different classifications of City of San José information assets:

Public

- Public information assets (data) should be destroyed when the data is no longer required for business purposes in accordance with the Records Retention and Disposition policy 6.1.5; however, there are no specific destruction requirements.

Sensitive

- Sensitive information assets (data) shall be destroyed when the data is no longer required for business purposes in accordance with the Records Retention and Disposition policy 6.1.5 and the Media Sanitization Standards set forth in section 8.6.4.

Confidential

Confidential information assets (data) shall be destroyed when the data is no longer required for business purposes in accordance with the Records Retention and Disposition policy 6.1.5 and the Media Sanitization Standards set forth in section 8.6.4. To ensure recovery of the information is impossible, the following specific destruction requirements apply:

- Data destruction via destroying physical media is an acceptable method.
- Data destruction via wiping with multiple passes is an acceptable method for appropriate types of media.
- A secure commercially-available method for data wiping is required.
- Data destruction via degaussing is an acceptable method for magnetic disk drives.
- Data destruction via degaussing is ***not*** an acceptable method for solid state media.
- Data destruction via reformatting of disk drives is ***not*** an acceptable method.
- Data destruction via deletion of encryption keys corresponding to encrypted data is ***not*** an acceptable method.
- Credit Card readers shall have all indications or input of Merchant ID (MID) and Cardholder Data (CHD) removed prior to surplus or return to vendor.

8.1.6 Data Inventory

Public

Public information assets have no inventory requirements.

Sensitive

Sensitive information assets (data) should be inventoried.

- The inventory should include: description of the data, physical location, associated servers, associated networks, and data owner.

Confidential

Confidential information assets (data) shall be inventoried.

- The inventory should include: description of the data, physical location, associated servers, associated networks, and data owner.
- The Confidential information asset (data) inventory shall be reviewed (at least annually, or as a result of significant change to the information system)
- All PII collected or stored shall include: intended use, whether it is shared, whom it is shared with (internally or externally), and a destroy date.

8.2 Mobile Computing Devices

Purpose – The City of San José recognizes the efficiency and customer service benefits of mobile devices where access supports critical municipal services. This is balanced with the stewardship of public resources, management of access outside of standard work hours, and employment rules under the Federal Fair Labor Standards Act. Therefore, the City of San José limits the authorization of mobile devices and stipends to circumstances where there are continuous and clear work gains identified by departments. Related, it is imperative that mobile devices used to conduct City of San José business be used appropriately, responsibly, and ethically.

Scope – The Mobile Device Policy applies to all users of City of San José information systems, networks, and information assets, including, but not limited to: full-time regular employees, part-time regular employees, temporary employees, elected officials, appointed officials, consultants, contractors, interns, and volunteers.

The policy applies to any mobile device used to access City resources, whether the device is owned by the user or by the City, and to all information and systems residing within the City's infrastructure or on hosted services.

8.2.1 Mobile Device Policy

The City of San José shall develop and maintain a Mobile Device Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among departments, and compliance. The Mobile Device Policy shall be reviewed at least annually, or as a result of significant change to the information system. All mobile device users shall abide by the Mobile Device Policy.

8.2.2 Mobile Device Configuration Requirements

All mobile devices connecting to or accessing the City of San José information systems shall meet the following configuration standards:

- Ability to run the City's selected Mobile Device Management (MDM) solution
- Ability to initiate remote wipe
- Ability to enable location tracking
- Ability to enumerate installed applications

- Ability to manipulate hardware
- Ability to enable complex device biometric/password/gesture lock
- Ability to restrict access to the device after maximum wrong password/gesture attempts
- Ability to run an approved device encryption solution
- Ability to run an approved malware protection solution

8.3 Personnel Security

Purpose - The City of San José Information Security Program relies upon people (users of the information system) to be responsible participants in maintaining system security. The risk of security incidents due to user action (whether unintentional or malicious) represent a significant risk to the information system. To minimize this risk, the City develops this Personnel Security standard which specifies security-related aspects of human resource management consistent with San José municipal code title 3 regarding personnel regulations.

Scope – This standard is applicable to all users of City of San José information systems including but not limited to full-time regular employees, part-time regular employees, temporary employees, consultants, contractors, and volunteers.

Impact – Attacks resulting from malicious insiders are the most damaging, widespread, and difficult to prevent/contain. It is important to understand and manage risk associated with individuals regarding:

- Required access to sensitive data
- Sensitive and business-critical job responsibilities
- Risky personal behavior
- Accumulation of excessive privilege
- Misuse and Disciplinary Actions

8.3.1 Monitoring of Personnel

The monitoring of individuals is coordinated with the management, legal, security, privacy, and human resource officials who conduct such monitoring. Monitoring is conducted in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

- Monitors logical access to information system to identify unauthorized actions.
- Monitors behavioral usage patterns to identify evidence of intruder compromise, insider threats, and risky behavior.
- Monitors user-installed software and user-initiated sharing for licensing/regulatory compliance.

8.3.2 Screening

Conducts screening prior to employment in accordance with established Human Resource policy and procedure.

8.3.3 Access Agreement

The City of San José requires all users to affirm acknowledgement and agreement to abide by policies and procedures set forth in the City Administrative Policy Manual including:

- 1.6.2 “Personal use of City Equipment,”
- 1.7.1 “Use of Email, Internet Services & Other Electronic Media,”
- 1.7.3 “Remote Access,”

- 1.7.4 “Cellular Telephone Policy,” and
- 1.7.6 “Information and Systems Security Policy.”

This affirmation must be on file with the Human Resources Department prior to provisioning any access to CSJ information systems.

8.3.4 Transfer/Termination

The City of San José shall establish procedures for reviewing and/or modifying access privileges of users to ensure that authentication and access privileges are updated in a timely fashion and to prevent accumulation of excessive privilege.

- Privileged user access to information systems shall be modified immediately when roles and responsibilities have changed.
- Supervisors are responsible for ensuring that appropriate access is provided to a user following a job change. The access should be consistent with the requirements for the new roles and responsibilities.
- An access modification request shall include the access to be removed and the access to be added.

Ensures accounts and access are terminated/disabled upon notification of termination.

The City of San José shall establish procedures for terminating the access privileges of users to ensure that authentication and access privileges are removed in a timely fashion.

- Privileged user access to information systems shall be removed immediately upon termination.
- The user’s manager or supervisor and the Department of Human Resources or Office of Employee Relations is responsible to ensure that appropriate requests are made so that access is immediately removed.
- All access for terminated users shall be deactivated immediately.
- Accounts for terminated users shall be disabled upon initial notification. In accordance with City Attorney's Office the account shall be deleted after the records retention period (720 days).

8.3.5 Discipline

Information and systems security is the responsibility of every employee of the City of San José. 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.

Disciplinary action shall be recommended for violation of policies in accordance with City of San José municipal code title 3 part 11 and the “Discipline Policy” section 2.1.3 of the City Administrative Policy Manual.

8.4 Awareness and Training

Purpose – The City of San José Information Security Program relies upon people (users of its information system) to act in accordance with established policy and procedure. There is a human element to nearly every security incident, which a vigilant and diligent security culture can combat. To minimize this risk, all users will be made aware of their responsibilities for protecting information and assets.

Scope – This standard is applicable to all users of City of San José information systems including but not limited to full-time regular employees, part-time regular employees, temporary employees, consultants, contractors, and volunteers.

Impact – Several security attack vectors target people, as an information system supported by a robust security policy is often much more difficult to compromise. Attacks like phishing, social engineering, card skimming, tailgating, and several others are difficult to prevent, requiring the participation of all users in prevention.

Security Awareness Training

All users shall be required to take a standard security and awareness training annually.

Elevated Privilege Training

Any users having or requesting elevated privileges (administrator access, root account, etc.) shall be required to take additional training detailing policies and responsibilities. The content should explain concepts including but not limited to: separation of elevated privilege accounts and standard accounts, principle of least privilege, data classification, and confidentiality requirements.

Executive Training

Senior executives shall be required to take additional training explaining the additional risk and need for extra diligence due to their status and influence within the City of San José. The content should explain concepts including but not limited to: spear-phishing, whaling, and social engineering.

Cybersecurity Training

Any users responsible for managing or responding to Cybersecurity incidents shall be required to take additional training detailing the responsibilities and procedures required to protect the City of San José information system and its users.

Incident Response Training

Any staff involved (or potentially involved) with resolving a service outage or security incident shall have appropriate training addressing security policies, incident response procedures, basic forensic investigation, and City of San José enterprise architecture overview.

PCI Training

Any staff involved (or potentially involved) with CardHolder Data transactions, systems, or components considered in scope for PCI shall have appropriate training addressing: security policies, secure configuration of devices, detection of tampering and skimming devices, storage and transmission of CHD, access controls, account and password policies,

Training Records

The City of San José shall retain an appropriate record of trainings, completion dates, and associated UserID. Successful completion of each training shall include an attestation that the user has read and understands the policies and procedures that have been presented to them as part of the training.

8.5 Physical Security

Purpose – Physical security involves security-in-depth, the use of multiple layers of interdependent systems such as physical barriers, Intrusion Detection Systems (IDS), Closed Circuit TeleVision (CCTV) surveillance, security guards, access control, lighting, etc. These techniques are designed to detect, deter, delay and/or deny unauthorized access to facilities, equipment, and resources. The City of San José shall perform periodic assessment of each physical environment where components of the information system reside to determine the minimum physical security safeguards necessary.

8.5.1 Physical Access Control

Monitors for unauthorized access and access patterns of authorized users.

8.5.2 Monitoring of Physical Environment

Monitors and alerts on off-nominal conditions involving access control and environmental control in any datacenter or facility where critical infrastructure is located.

8.5.3 Emergency Procedures

Ensures updated emergency procedures in conjunction with the Employee Emergency Response Team (EERT) for facilities.

Ensures emergency lighting and emergency shutoff procedures in any datacenter or facility where critical infrastructure is located.

8.5.4 Environmental Controls

Protects the information system from threats involving loss of power, fire, water (flood, humidity), temperature (hot and cold) in any datacenter or facility where critical infrastructure is located.

8.6 Media Protection

Purpose – External media used for data storage represents a significant risk to the confidentiality and integrity of information assets (data). Sensitive data may be leaked or malicious data may be introduced into the information system. The Media Protection Standard provides requirements for the safe handling of various types of media.

Scope – This standard applies to all users of City of San José information systems, networks, and information assets (including but not limited to full-time regular employees, part-time regular employees, temporary employees, consultants, contractors and volunteers).

This standard applies to City of San José information systems, networks, and information assets (whether located onsite or at off-site locations).

External media devices include but are not limited to:

- Optical disc media (CD-ROM, DVD-ROM, BD-ROM)
- Magnetic disk media (floppy disks, portable hard drives, tapes, digital video disks)
- Flash memory media (thumb drives, SSD hard drives)
- Portable computers (laptops, tablets, smartphones)
- Hardcopy (paper, photographs, microfilm, transparencies)

8.6.1 Media Marking

All external media containing sensitive or confidential information shall be marked to indicate the classification of data it contains.

8.6.2 Media Storage

All external media containing sensitive or confidential information shall be kept in possession of an individual authorized to access it.

All external media containing sensitive or confidential information shall be stored in a locked container when not in use.

8.6.3 Media Transport

In accordance with City of San José Administrative Policy Manual section 1.7.6, data stored on non-City systems or portable devices (such as laptops, CDs, USB memory sticks, etc.) shall be encrypted. Further, use of encryption technologies shall comply with Cryptography standards set forth in section 9.6.

Media containing public or sensitive data should not be transported offsite unless necessary for business purposes.

Media containing confidential data shall be encrypted (using encryption mechanisms approved by the Cryptography standards set forth in section 9.6) when it is stored on external media. The physical devices (e.g. backup tapes, CD-ROM) containing encrypted confidential data shall be appropriately logged and sent via secured courier or other delivery method that can be tracked.

8.6.4 Media Sanitization and Reuse

All external media containing sensitive or confidential information shall be appropriately sanitized prior to disposal or reuse. A non-destructive secure erase method is appropriate where media will be reused, whereas a destructive degaussing operation is appropriate prior to disposal. Neither 1-pass secure “wipe” nor “quick format” (i.e. deletion of partition table, boot record, etc.) shall be sufficient for reuse of media as free space can retain recoverable information. Deletion of encryption keys corresponding to encrypted data shall not be considered a method of secure destruction.

8.7 Incident Response

Purpose – The City of San José depends on critical information systems and technologies to process and manage data, transactions, audits, and reporting to deliver uninterrupted services on behalf of internal employees and the general public.

The Incident Response Standard defines the structure, approach, and requirements which shall be documented and maintained in the Incident Response Plan.

Scope – The City of San José Incident Response capability is applicable to information systems, networks, and information assets (whether located onsite or at off-site locations).

8.7.1 Incident Response Training

See section 8.4 Awareness and Training

8.7.2 Incident Categorization

The severity level given to an incident will be determined by scale of impact (3-low, 2-medium, or 1-high) to citywide services in conjunction with risk factor (3-low, 2-medium, or 1-high).

Incident Severity			Risk		
			3 - Low Issue prevents the user from performing a portion of their duties.	2 - Medium Issue prevents the user from performing critical time sensitive functions	1 - High Service or major portion of a service is unavailable
Impact	3 - Low	• One or two personnel • Degraded Service Levels but still processing within SLA constraints	3 - Low	3 - Low	2 - Medium
	2 - Medium	• Multiple personnel in one physical location • Degraded Service Levels causing service to fall below SLA or able to perform only minimum level of service • It appears cause of incident falls across multiple functional areas	2 - Medium	2 - Medium	1 - High
	1 - High	• All users of a specific service • Personnel from multiple departments are affected • Public facing service is unavailable • Services that are directly impacting public safety	1 - High	1 - High	1 - High

8.7.3 Incident Handling

When a severity (1 – High) incident occurs, Customer Care will activate a call bridge for incident response. All IT service providers Team Manager (or his/her proxy) and IT Executives must join the Bridge (see below). Team Manager of the impacted service must take lead to identify root cause and restore service as quickly as possible.

- Call in number: 877-873-8017
- Passcode: 1561039

During the incident handling process, focus will be on containment, eradication, and mitigation of any new or residual vulnerabilities.

8.7.4 Incident Reporting

All actions taken during the phases of incident response: detection, containment, eradication, and recovery) shall be documented. An accurate record of observations, systems affected, commands issued, timestamps, and persons involved is critical- especially if the incident leads to a criminal investigation.

For minor malware infections and service outages, a Team Manager (or assigned proxy) must complete an incident report within twenty-four (24) hours of incident resolution and post to ITD SharePoint site:

- SharePoint -> ITD Operations -> Incident Management -> Incidents

For more significant security incidents impacting multiple systems, the Cybersecurity team shall complete an incident report including any relevant forensic evidence and post to the SIRS site on SharePoint:

- SharePoint -> Information Security Office -> SIRS

8.7.5 Postmortem

Subsequent to the occurrence of any security incident, a review session shall be conducted. All Team Managers (or assigned proxy) must attend. Agenda shall include:

- Present Root Cause Analysis
- Remediation steps to restore service
- What steps are being taken to prevent reoccurrence

For higher severity incidents, a postmortem meeting shall be scheduled with the following Stakeholders:

- Severity 1 – Exec Team/Division Manager(s)
- Severity 2 – Division Manager(s)/Team Managers

8.8 Maintenance

Purpose – The City of San José must ensure that all components of its information system remain in a secure and operational state. This standard for ongoing maintenance of information system components will ensure routine, controlled, and scheduled maintenance activities.

Scope – This standard applies to all City of San José information systems, networks, and information assets.

Impact – By implementing a comprehensive maintenance plan that addresses hardware, applications, and operating systems, failures can be minimized, the scope of supported devices and configurations can be controlled, and costs can be optimized.

8.8.1 Maintenance Plan

A maintenance plan should be developed for each Information System and include the following items (at a minimum).

Notification of Planned Maintenance Windows

The City of San José shall ensure that a standard notification is sent to all users that are potentially impacted by a service outage caused by scheduled maintenance.

Off-site Maintenance

All information system components that are removed from City control must be evaluated for potential tampering or unauthorized modification prior to returning to operation within the information system.

Remote Maintenance

Any maintenance conducted remotely by a third party must be supervised for the duration of the maintenance period. Any temporary access that is granted to facilitate remote maintenance shall be terminated immediately following the maintenance period.

Preventative Maintenance

The City of San José shall ensure that each classification of information security component has an associated lifecycle duration, and that components are proactively maintained until they reach end-of-life.

End of Maintenance

The City of San José shall ensure that each classification of information security component has an associated end-of-life date, after which the system will be either migrated to a supported system or retired for disposal.

8.8.2 Application Maintenance

The City of San José shall ensure that applications are proactively maintained with vendor supplied enhancements and/or security fixes. Once the vendor no longer supports the application or the system end-of-life is reached, its use should be discontinued.

8.8.3 Operating System Maintenance

The City of San José shall ensure that operating systems are proactively maintained with vendor supplied enhancements and/or security fixes. Once the vendor no longer supports the application or the system end-of-life is reached, its use should be discontinued.

8.8.4 Hardware Maintenance

The City of San José shall ensure that hardware is proactively maintained with vendor supplied enhancements and/or security fixes. Once the vendor no longer supports the hardware or the system end-of-life is reached, its use should be discontinued.

9 Technical Controls

This section specifies the security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

9.1 Identification and Authentication

Purpose – The City of San José must ensure that all individuals are uniquely identified, and moreover once access is granted to an individual, the intended individual is truly the one accessing the system. Management and verification of the identity of users and their access to systems and applications

Scope – This standard applies to all users of City of San José information systems, networks, and information assets (including but not limited to full-time regular employees, part-time regular employees, temporary employees, consultants, contractors, and volunteers).

9.1.1 User Identification and Authentication

Username

Usernames/userids shall be uniquely assigned in the format of given name [dot] surname. In case of conflict with an existing username/userid, a middle initial or trailing digit may be added to provide uniqueness.

ID Number

Employee ID numbers shall be uniquely assigned in the format of xxxxxx where x is a digit zero (0) through nine (9).

Password

Passwords shall meet each of the following minimum requirements:

- Must be eight (8) characters in length
- Must contain at least one (1) lower case letter
- Must contain at least one (1) upper case letter
- Must contain at least one (1) number
- Must contain at least one (1) punctuation “special” character
- Must be different from the previous four (4) passwords
- If a CJIS or PCI system, it must be changed every 90 days; City systems do not require password change unless it is suspected of being compromised
- Temporary (first time use) passwords must be set to a unique value for each user
- Temporary passwords must be changed upon first logon
- Must not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Must not be comprised of an obvious keyboard sequence (i.e., QWERTY)
- Must not include "guessable" data such as personal information about the user

Prohibited dictionary words and keyboard sequences

Passwords less than 14 characters in length shall not contain the following:

- 000000
- 111111
- 112233
- 123456
- 1qaz2wsx
- 3154061
- 456a33
- 66936455
- 789_234
- aaaaaa
- abc123
- admin
- career
- carrier
- comdy
- cheer

- cheezy
- default
- Exigent
- letmein
- old123ma
- opensesame
- passw0rd
- p@ssw0rd
- password
- penis
- qwerty
- snowman
- soccer
- student
- welcome
- !qaz1qaz

Biometrics

Biometric authentication shall be enabled only after identity verification and a reasonable assurance that the biometric factor is both authentic and unique to the individual.

9.1.2 Device Identification and Authentication

The following types of devices shall be required to be identified and authenticated prior to granting access to City of San José information systems:

- Any device connecting to secure network
- Any device accessing CardHolder Data or PCI systems
- Any device accessing CJI or CJIS systems

9.1.3 Multi-Factor Authentication (MFA)

Multi-Factor Authentication is defined as an authentication mechanism using two or more different factors to achieve authentication. Factors include: something you know (e.g., password, passphrase, PIN), something you have (e.g., badge, token, cryptographic identification device), and something you are (e.g., biometric).

- The City of San José shall ensure that any privileged access is granted only upon successful verification of two (2) factors.
- The City of San José shall ensure that remote access (i.e. VPN) is granted only upon successful verification of two (2) factors.

9.2 Access Controls

Purpose – The objective of this standard is to outline the information security requirements for managing risks associated with unauthorized and inappropriate user access. Using access management, the City of San José shall provide access to all members of its workforce in as efficient and effective manner as possible while protecting against unauthorized access, the loss or corruption of systems, applications, and data.

Scope – This standard applies to all users of City of San José information systems, networks and information assets (including but not limited to full-time regular employees, part-time regular employees, temporary employees, consultants, contractors and volunteers).

This standard applies to City of San José information systems, networks, and information assets (whether located onsite or at off-site locations).

Public access to City of San José publicly accessible systems, such as City of San José websites or public web applications are specifically excluded from this standard.

Exceptions – Exceptions to this policy shall be documented, reviewed, and authorized by the City Information Security Officer (CISO).

9.2.1 Access Request

- The City of San José shall establish procedures to request access to City of San José information systems, networks and information assets that records and tracks requests from inception through provisioning of access.
- For City of San José employees or contractors, access requests are made by the employee or contractor using the established procedure.
- For third party requestors (e.g. vendors, suppliers), requests are made by the City of San José sponsoring department on behalf of the Third Party.

9.2.2 Access Authorization

- Access to City of San José information systems, networks and information assets must be granted under the Principle of Least Privilege. Authorized access must provide the least access required for the requestor to perform their job function.
- For City of San José employees and contractors, the requestor's manager or supervisor and Human Resources (for new hire) must verify the requestor's identity.
- For City of San José employees and contractors, the requestor's immediate manager or supervisor and Department Director (or designee) must review and authorize access requests prior to access being granted. For City of San José Third Party access, the sponsoring City of San José business group lead (or designee) must review and authorize access requests prior to access being granted.
- Rejected access requests must be appropriately documented. This documentation must include the reasons for the rejection.

9.2.3 Access Provisioning

- Access is provisioned only by authorized City of San José employees or contractors
- Access is provisioned only for the access that was authorized
- User access must be provisioned based upon job classification and function. (also known as Role-Based Access Control (RBAC))
- Access is only provisioned once the requestor has acknowledged the provisions set forth in section 8.3.3.
- Access for Contractors and Third Parties must expire and require re-authorization within 180 days

9.2.4 *Network Authentication*

User's workstations and laptops must be configured to request Microsoft Active Directory TM domain authentication (network logon) at startup. If the domain is not available or authentication for some reason cannot occur, then the machine shall not be permitted to access the network. The machine shall not cache more than 7 logons before requiring re-authentication from a domain controller.

9.2.5 *Separation of Duties*

The City of San José shall separate duties of individuals to prevent the potential for abuse of authorized privileges and to reduce the risk of malevolent activity without collusion. 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.
- Duties shall also be distributed such that no individual is the only one capable of performing critical functions or executing critical procedures.
- Information system access authorizations shall support separation of duties via a chain of approvals.

9.2.6 *Privileged User Access*

The term "privileged user account" can be used to describe any account that gives non-restrictive access to the system. Such accounts provide users with the ability to access and modify critical system settings, view restricted data, etc. The higher the privileges of the account, the more valuable it is to an attacker. What makes privileged accounts dangerous is not the extent of their access, but rather how easy it is for them to perform malicious action and how hard it can be to detect. By limiting user privileges, there are fewer avenues for attackers.

- Users with privileged access to information systems, network devices or information assets must be authenticated using approved authentication systems.
- Default, Shared and Generic privileged accounts are not permitted unless an exception is granted by the City of San José Information Technology Department (ITD).
- Privileged access to systems must be based on a valid and unique user identity.
- Privileged accounts for each user must be created using a standard format.

9.2.7 *Inactive Accounts*

- Accounts which are inactive more than ninety (90) days shall be disabled.

9.2.8 *Failed Logon Attempts*

- In order to guard against password-guessing and brute-force attempts, access management configurations will lock a user's account after 5 unsuccessful login attempts.
- In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password was incorrect.

9.2.9 *Password Confidentiality*

Passwords are confidential and should be treated with the same discretion as any confidential City of San José information assets. Users are required to adhere to the following requirements:

- Users must not disclose their passwords to anyone.

- Users must not share their passwords with others (co-workers, supervisors, family, etc.).
- Users must not write down their passwords.
- Users must not check the "save password" box when authenticating to applications and web sites.
- Users must not send passwords via email.
- Users must never save their passwords in any unencrypted file (password protected file is not the same as an encrypted file).
- New and reset passwords are to be unique per user and changed immediately after first use.

Wherever systems software permits, the display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties are unable to observe, record, or recover them.

9.2.10 Credential Compromise

Users must immediately report any suspicious activity involving a password to City of San José Information Technology Department (ITD). Any request for passwords over the phone or email, whether the request came from within the City of San José or not, must be reported. When a password is suspected to have been compromised the user passwords must be changed.

9.2.11 Session Lock

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. These mechanisms may also be automated in case the user forgets to initiate the session lock.

- The information system shall prevent further access to the system by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a request from a user.
- The session lock shall be retained until the user reestablishes access using established identification and authentication procedures.
- The grace period for delaying automated session lock shall be no longer than seven (7) seconds.

9.2.12 Password Reset

- The City of San José shall establish a password reset procedure to restore locked user accounts.
- The password reset procedure shall be documented such that multiple authorized individuals can execute the procedure.
- The password reset procedure shall include verification of the user’s identity prior to distributing the new password.

9.2.13 UNIX/LINUX System Access

- UNIX/Linux systems must be configured to prevent direct logon to the “root” account. Initial logon must use a userid that identifies a specific user. If such users have been granted the ability to achieve super-user privileges, they may then "set_userid" ("su") to gain "root" access.
- UNIX/Linux system logs must record all “set_userid" ("su") to gain "root" access
- UNIX/Linux file permissions must be set to only provide the access required for a user to perform their job function

9.2.14 Remote Network Access

- Remote access to City of San José networks shall use multi-factor authentication, validating at least two factors (such as smart cards, certificates, or biometrics).

- Remote access to City of San José networks is only allowed using City of San José approved remote access technologies.

9.2.15 System Use Notification

The system shall display to users a notification banner before granting access to the system that provides privacy and security notices consistent with applicable laws, City policy, and standards which states that:

- Users are accessing a City of San José information system;
- Information system usage may be monitored, recorded, and subject to audit;
- Unauthorized use of the information system is prohibited and subject to criminal and civil penalties;
- Use of the information system indicates consent to monitoring and recording;

The system shall retain the notification banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

For publicly accessible systems:

- Displays system use information before granting further access;
- Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities;
- Includes a description of the authorized uses of the system.

9.3 Audit Logging

Purpose – The City of San José would like to ensure that the IT department can detect and prevent off-nominal conditions to minimize disruptions to the information system. To support the investigation and response to potentially disruptive incidents, this standard shall specify system level audit logging and alerting requirements. As system audit log data describes and identifies individual user activities, its collection (or correlation) will often constitute PII, which the City of San José must protect appropriately. This standard shall also specify protection mechanisms for sensitive audit log data.

Scope – This standard applies to every technology asset belonging to the City of San José capable of producing diagnostic logging information. These logs shall be captured, retained, and protected for inspection and/or analysis.

Impact – If audit settings are not configured or are not complete enough, security incidents might go undetected or analysis will be incomplete to identify and subsequently prevent security incidents. If audit settings are overly enabled, critically important entries in the system logs may be obscured by meaningless entries or available data storage may be exhausted.

9.3.1 Logging

Audited Events – All City of San José technology assets shall be configured to log the following event types (as possible):

Windows

- Audit Credential Validation – Success, Failure
- Audit Computer Account Management – Success

- Audit Other Account Management Events – Success, Failure
- Audit Security Group Management – Success, Failure
- Audit User Account Management – Success, Failure
- Audit Account Lockout – Success
- Audit Logoff – Success
- Audit Logon – Success, Failure
- Audit Audit Policy Change – Success, Failure
- Audit Authentication Policy Change – Success
- Audit Other System Events – Success, Failure
- Audit Security State Change – Success, Failure
- Audit System Integrity – Success, Failure

Other Devices and Operating Systems

- Failed user logons (*nix syslog, sshd)
- Audit logs were cleared
- Account creation/deletion
- Group membership
- Use of elevated privilege (*nix sudo/su log)

Application

- Client requests and server responses
- Account information such as successful and failed authentication attempts, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges
- Usage information such as the number of transactions occurring in a certain period (e.g., minute, hour) and the size of transactions (e.g., e-mail message size, file transfer size)
- Significant operational actions such as application startup and shutdown, application failures, and major application configuration changes

New Device Selection – Prior to selection of equipment vendor, devices, configuration, etc. the audit logging capabilities should be evaluated and aligned with the auditing goals specified by this standard.

Audit Failures – The system shall be configured to send an alert to the appropriate IT team to notify that audit logs are no longer being received.

9.3.2 Logging Capacity

Centralized log collection servers shall be configured with sufficient storage to retain audit log data in accordance with approved record retention schedules. The logging capacity for individual components should be set for circular (overwrite as needed) if they are configured to forward audit log data to a centralized log server.

9.3.3 Logging Review

A logging policy review shall be conducted at least annually to verify relevance and ability to support after the fact investigation of events. The following areas shall be considered:

- List of audited events

- Logging capacity
- Logs provided by external providers
- Recommendations gathered from lessons learned during Incident Response

9.3.4 Time Stamps

All information system components shall be configured to synchronize their time with authoritative sources on a regular basis so that timestamps in audit logs are consistent. Where applicable, logging mechanisms shall be configured to include timestamps when this is not the default configuration.

9.3.5 Protection of Logs

All information system components capable of producing logs shall be configured to require authentication via a privileged account before viewing, modifying, or deleting audit log data. Audit log data shall be transmitted in a secure manner only to approved log collection servers.

9.3.6 External Provider Logs

Where available, external provider audit log data shall be collected for inspection and/or analysis. Agreements shall be put in place to ensure audit log data is protected at the same or a greater level than internal audit log data as described in this standard.

9.4 Systems and Network Communications Security

Purpose – Properly securing networks and communication systems requires a comprehensive and layered approach. In order to protect information systems, users, and information assets (data), the City of San José implements a wide range of protection mechanisms to prevent unauthorized access, modification, use, disclosure, or disruption. The Systems and Network Communications Security Standard provides requirements for the protection of communications and communication devices.

Scope – This standard applies to City of San José information systems, networks, and information assets (whether located onsite or at off-site locations).

9.4.1 Network Segmentation

Logically separates the network to provide a defense in depth approach to protecting the information system.

- Any systems exposed to the public Internet shall be placed in a DMZ which is segmented from the internal network.
- All wireless networks shall be segmented from PCI and CJIS networks.

9.4.2 Denial of Service (DoS) Mitigation

Maintains the capability to minimize the impact of DoS and Distributed DoS (DDoS) attacks including reflection, amplification, flooding, and botnets.

9.4.3 Resource Availability

Designs network and systems in support of critical resources in order to meet availability goals.

9.4.4 Boundary Protection

Monitoring and filtering capability shall be present at each system boundary. System boundaries shall be clearly defined per system. Internet and DMZ zones shall be considered boundaries.

9.4.5 Session Timeout

Disconnects idle connections after no more than four (4) hours for VPN and network connections. PCI systems must disconnect after 15 minutes of inactivity. CJIS systems must disconnect after 30 minutes of inactivity. Elevated privilege sessions must disconnect after 15 minutes. Application sessions must disconnect after 30 minutes of inactivity.

9.4.6 Certificates

The City of San José ensures all certificates are valid and proactively renews or replaces them prior to expiration.

- Certificates must not be self-signed.
- Certificates must link to a trusted Certificate Authority (CA).
- Certificates must support TLS version 1.2 or higher.
- Certificates must support SHA2 or higher.
- The certificate should be capable of validation via Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP).

9.4.7 Voice over Internet Protocol (VoIP)

To ensure quality of service, network traffic is prioritized and segregated to support the availability of VoIP services. Limitation and usage restrictions for VoIP technologies are implemented based on the potential to cause damage to the information system if used maliciously. Use of VoIP including traffic volume and patterns within the information system are monitored to identify unauthorized or malicious activity.

9.4.8 Name Address Resolution

The City of San José ensures the availability and integrity of Domain Name System (DNS) servers to protect critical services, applications, and infrastructure.

Segmentation

- The DNS service shall separate internal and external functions.
- Publicly accessible external nameservers shall be authoritative-only, not recursive.
- External nameservers should contain only publicly accessible zones, not internal zones.
- The DNS service should maintain least functionality to limit attack surface (i.e., if nameservers are serving authoritative data, they should not also be serving as recursive servers).

Availability

- The DNS service shall be highly available such that if one fails, another can assume the load.
- The DNS service should be distributed to improve performance such that branch offices have both recursive and authoritative nameservers on-site to serve those locations.

Hidden Primary

- The servers that host the master copy of any zone should be hidden primaries (i.e., The primary servers only exist to serve data to the secondary nameservers throughout the organization; they are not listed as nameservers for any zone, and they are not accessible to any end-user. This helps to ensure the integrity of DNS data by limiting access to the primary nameservers to just those individuals responsible for the maintenance of the servers and the data that resides on them).

Rate Limiting

- DNS servers should use Response Rate Limiting (RRL) to throttle the speed at which an authoritative name server answers queries from a particular IP address (i.e., To prevent many types of DDoS attack, a name server uses RRL to remember how many times it has sent the same response to the same querier. If this rate exceeds a threshold, the name server waits for a time before sending a response).

Access Control

- All traffic to the nameservers should be restricted to ensure they process and respond only to DNS traffic (i.e., on-server Access Control Lists (ACLs) and firewall ACLs).
- Zone transfers should be protected by access controls as well as transaction signatures (TSIGs) (i.e., on-server Access Control Lists (ACLs) and firewall ACLs).
- Secondary servers should deny all zone transfer requests.

Active Directory Integrated DNS

- To improve security and simplify zone replication, at least one domain controller (DC) should also be a DNS server.
- To protect proper replication, If multiple DCs are configured as DNS servers, they should be configured to use each other for resolution first and themselves second.
- To protect availability, all domain-joined computers shall use only internal DNS servers.
- In a multi-site environment, domain members should be configured to use the DNS servers at their local site before those at a different site.
- AD-integrated zones shall use only secure dynamic updates.
- Configure aging and scavenging to avoid stale DNS records.

9.4.9 Wireless Network Security

Isolates wireless network traffic from internal networks with the exception of the secured *Private WiFi* project. Ensures secure communications via Wifi Protected Access (WPA) version 2 and prohibits Wireless Equivalency Protocol (WEP). Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.

Per PCI DSS 1.2.3 all wireless traffic shall be segmented from the CHD environment.

9.4.10 Restricted Ports, Protocols, and Services

The City of San José documents, enforces, and reviews the following list of specifically prohibited network ports, protocols, and services that are disabled and/or blocked from the information system.

- 21: cleartext File Transfer Protocol (FTP)
- 23: unencrypted telnet
- Secure Shell (SSH) < version 2
- Secure Socket Layer (SSL) all versions
- Server Message Block (SMB) version 1

- Common Internet File System (CIFS)
- Message Digest version 5 (MD5)
- Data Encryption Standard (DES)
- Wired Equivalency Protocol (WEP)

9.5 System Integrity

Purpose – Maintaining integrity of an information system ensures predictable and reliable continued operation. The System Integrity Standard provides requirements for maintaining the integrity of information system components including: remediation of vulnerabilities, protection from malicious code, protection of email communications, and preventing manipulation of input handling.

Scope – This standard applies to City of San José information systems, networks, and information assets (whether located onsite or at off-site locations).

9.5.1 Vulnerability Remediation

The City of San José implements a vulnerability severity rating scale consisting of:

- Critical – currently or imminently impacting systems, services, users, or having a city-wide impact
- High – potential to impact multiple systems, services, users or potentially have a city-wide impact
- Moderate – potential to impact a small group of systems, services, or users
- Low – impact to a single system, service, or user
- None – no impact or risk accepted

Vulnerability scans shall be conducted at an interval specified in section 7.7.4 and used to remediate vulnerabilities with the following goals:

- Critical – immediately; no more than seven (7) days
- High – one (1) month
- Moderate – two (2) months
- Low – three (3) months
- Informational – no action or risk accepted

9.5.2 Malicious Code Protection

Ensure every City of San José asset is protected by the currently adopted malicious code protection solution. Makes available a version for personal use, which is required on any device prior to initiating remote connection.

9.5.3 Email Protection

The City of San José shall combat unsolicited bulk email (Spam) in compliance with mandates such as California Business and Professions Code (Sections 17529 & 22948), and the federal CAN-SPAM Act. The information system shall ensure spam detection and prevention countermeasures are available and functional. Such countermeasure solutions shall be automatically kept current as updated protections are made available. Email containing sensitive and confidential data shall be encrypted.

Email services shall be configured to minimize the processing of illegitimate email.

- Configure Email Anti-Spam Protection policies for your organization.

- Email servers shall be configured to prevent open relay; emails sent through City of San José servers shall have domains owned by City of San José only.
- Turn on audit logging for all user mailboxes.
- Configure Sender Policy Framework (SPF) to validate outbound email sent from your domain.
- Configure DomainKeys Identified Mail (DKIM) to ensure that destination email systems trust messages sent from your domain.
- Implement Domain-based Message Authentication, Reporting, and Conformance (DMARC) for outbound mail to authenticate mail senders and ensure that destination email systems trust messages sent from your domain.

9.5.4 Input Checking

Performs application-level scans to ensure input fields handle out-of-bounds and erroneous conditions gracefully and do not lead to vulnerabilities in the underlying application or system.

9.6 Cryptography

Purpose – The City of San José contains information systems that process and store information assets (data) on behalf of internal employees and the public. Securing information of a personal, sensitive, or secretive nature is of paramount importance. This importance extends to the City of San José for purposes of protecting information assets (data) and privacy. This Cryptography Standard provides requirements for the implementation and use of cryptographic processes (including encryption, cyphers, hashing, key-based information exchanges) within information systems and networks. This Cryptography Standard also provides requirements for the selection and management of encryption technologies.

Scope – This standard applies to all users of City of San José information systems, networks, and information assets (including but not limited to full-time regular employees, part-time regular employees, temporary employees, consultants, contractors, and volunteers).

This standard applies to City of San José information systems, networks, and information assets (whether located onsite or at off-site locations).

Impact – The loss of confidentiality to sensitive information may constitute a data breach, violation of privacy, failure to comply with regulations, or negligence of duty. The City of San José could face: penalties, monetary fines, loss of compliance/certification, damage to reputation, and/or lawsuits for failing to adequately protect information assets (data) and privacy.

9.6.1 Application of Encryption

Passwords must be encrypted and/or rendered unreadable as follows:

- Passwords must be rendered unreadable by one way hash when stored on disk
- Passwords must be rendered unreadable when transmitted over a network (both City of San José internal networks and over public networks)

All non-console administrative access must be encrypted using technologies such as TLS, SSH, or VPN for web-based management and other non-console administrative access.

9.6.2 Unauthorized Encryption

The use of encryption for purposes other than those expressly permitted in this standard must be authorized by the City Information Security Officer (CISO). Unauthorized use of encryption may result in disciplinary action.

Encryption technologies that have been "broken," or deemed no longer cryptographically sound, shall be added to the list of restricted ports, protocols, and services as specified in standard section 9.4.10.

9.6.3 Encryption Technology

Encryption technologies employed by the City of San José must be robust and kept in line with recognized standards, taking into account changes in technology and advances in encryption.

- Encryption technologies shall be approved by the City of San José Information Technology Department (ITD) prior to authorized implementation.
- The use of encryption shall be limited to algorithms that have received public review and have been proven to work effectively.
- The use of proprietary encryption algorithms is prohibited for any use.

Key Management

Employed encryption technologies that require cryptographic keys must have well-documented and accepted key management procedures. These procedures must satisfy the following requirements:

- Symmetric cryptographic keys shall be changed at least annually or as deemed necessary by CSJ Information Technology Department (ITD).
- Cryptographic keys that have either been compromised or are suspected of being compromised must be revoked immediately.
- Cryptographic keys shall have an expiration date.
- Cryptographic keys shall not be re-used once revoked or expired.
- Cryptographic keys shall be assigned to an individual responsible for protecting integrity and confidentiality.
- Sharing of cryptographic keys shall be authorized only after approval and restricted to the fewest number of individuals necessary.
- The distribution of cryptographic keys shall ensure confidentiality and integrity of the keys.
- The storage of cryptographic keys shall ensure confidentiality and integrity of the keys.
- The unauthorized substitution of cryptographic keys shall be prevented.
- Cryptographic keys shall only be generated on a centralized secured system by the Information Technology Department (ITD).

Digital Certificates

The use of digital certificates within the City of San José must adhere to City of San José Digital Certificate standards based on NIST 800-175b section 5.2.3 PKI. City of San José Certificate and PKI solutions must be approved by the City of San José Information Technology Department (ITD).

Compliance with Legislation and Regulation

The use of encryption must comply with appropriate country, state, and local legislation and regulation. This includes all import and export law.

10 References

None available at this time.

11 Glossary/Acronyms

Term	Definition
Authentication	The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.
Fail-Over or Recovery Scenarios	A set of resulting situations or conditions based on an unspecified event that defines the recovery, fail-over and restoration requirements and situations for the critical services supplied.
Departmental or Recovery Teams	Teams of specific key managers or personnel designated to execute the recovery or continuity of critical services from one condition or location to a secondary state or back-up location.
Encryption	The process of encoding information in such a way that it is not easily readable. The encryption process makes use of an algorithm also called a cipher.
Common Internet File System (CIFS)	CIFS is a Microsoft proprietary implementation of the Server Message Block (SMB) protocol that was used in legacy versions of Windows prior to Windows Vista (2006).
Cryptography	The practice and study of techniques for secure communication that protects it from third parties. Cryptographic processes include encryption, hashing, and key exchange.
Information Asset	A definable piece of information regardless of format, which is recognized as valuable to the organization. May also be referred to as data.
Information System (IS)	An organized system for collecting, creating, storing, processing, and distributing information, consisting of hardware, software, data, business process and people.
Internet Service Provider (ISP)	An organization that provides services for accessing, using, or participating in the Internet.
Network	A group of two or more devices that can communicate with each other.
Policy	A set of directional statements and requirements aiming to protect corporate values, assets, and intelligence. Policies serve as the foundation for related standards, procedures, and guidelines.
Recovery Point Objective (RPO)	The amount of data (measured in time, e.g., hours) that can be lost following an unplanned interruption, which represents the time at which data must be restored in order to resume processing transactions. RPO is the basis on which a data protection strategy (data backup and recovery) is developed.
Recovery Timeframe Objective (RTO)	The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTOs are often used as the basis for the development of recovery strategies, and as a determinant of whether to implement the recovery strategies during a disaster situation. Similar Terms: Maximum Allowable Downtime (MAD) or Maximum Allowable Outage (MAO)
Server Message Block (SMB)	SMB is a file sharing protocol that was invented by IBM designed to allow computers to read and write files to a remote host over a Local Area Network (LAN).

Term	Definition
Service Level Agreement (SLA)	A formal or informal contract or agreement between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. The SLA defines level of services the customer can expect to receive. May also be referred to as Memorandum Of Understanding (MOU) or Memorandum Of Agreement (MOA)
Standard Operating Procedure (SOP)	A set of defined instructions for implementing specific policy requirements and executing standard practices. May also be referred to as a playbook.
Storage Media	Any technology, including devices and materials, used to place, keep, and retrieve electronic data or information.
Third Party	Any individual or entity that is not a member of the organization's workforce. A Third Party generally is a person or entity that performs specific functions or activities on behalf of the organization, or provides services to the organization under a contract or agreement with the organization.
Transport Layer Security (TLS)	TLS provides a protected channel for sending data between a server and a client. TLS protects the application data by using a set of cryptographic algorithms to ensure the confidentiality, integrity, and authenticity of exchanged application data.
Workforce	The individuals engaged in work for the organization which includes employees, volunteers, trainees, contractors, and other persons directed by the organization in the performance of specific work responsibilities.

12 Document Change History

Author	Version	Date	Changes
Marcelo Peredo	0.01	June 2018	Initial version
Ed Walker	0.99	Oct 2018	Add content; change formatting; renumber sections; add NIST control mapping; update definitions
Marcelo Peredo	1.0	November 2018	Accepted changes; removed comments; prepared for IT Leadership feedback.
Ed Walker	1.1	December 2018	Change to sections 5.4, 5.6.1, 5.6.2, 5.6.3, 5.6.4, 5.7.4, 6.1.2, 6.1.3, 6.1.4 Added section 5.4.3 Correct numbering 5.2.1, 5.2.2
Marcelo Peredo	1.2	January 2019	Added section Security Objectives and Security Guiding Principles. Added header and footer to document
Ed Walker	1.3	June 2019	Cybersecurity team annual review. Align with City Security Policy 1.7.6: • Globally replace “Internal” data classification with “Sensitive” • align content in section 2 • align content in section 8.3.3 • align content in section 8.3.5 • align content in section 9.2.5 Align with City Records Retention and Disposition policy 6.1.5 in: • section 8.1.5 • section 8.3.4 • section 9.3.2 Align with PCI requirements in: • new sections 7.2.15.x • section 7.7.5 • section 8.4 • section 9.4.1 • section 9.4.5 • section 9.4.9 Correct numbering in: • section 7.2.15 • section 7.3 • section 7.6.1 • section 8.1.5 • section 8.7.1 completed description in section 4; minor rewording section 7.6.3; update content in section 7.4 to align with other documents; add section 7.4.4 as a separate control; minor

			rewording section 8.1; section 8.7.4 add additional process; add sections 8.8.1 – 8.8.4; section 9.1.1 change to 180 days; minor rewording section 9.2; section 9.2.7 change to 90 days; section 9.2.11 change to 15 min; minor rewording section 9.2.14; add application logging & remove process creation from section 9.3.1; add prohibited protocols in section 9.4.10; change remediation requirements 9.5.1; remove redundancy in section 9.6.1
Ed Walker	1.3	November 2021	minor rewording section 8.1; add detail & formatting section 8.3.1; streamline formatting section 9.1.3; minor rewording & formatting section 9.4.8
Marcelo Peredo	1.3	December 2021	Incorporated modifications on roles and responsibilities based on City Auditor's feedback. Section 3. Changed section 9.1.1 to reflect new password requirements. Changed 7.7.4 Vulnerability Scanning frequency to quarterly.

Appendix A: List of Controls (NIST 800-53 rev 4)

Control Families

AC - Access Control
AU - Audit and Accountability
AT - Awareness and Training
CM - Configuration Management
CP - Contingency Planning
IA - Identification and Authentication
IR - Incident Response
MA - Maintenance
MP - Media Protection
PS - Personnel Security
PE - Physical and Environmental Protection
PL - Planning
PM - Program Management
RA - Risk Assessment
CA - Security Assessment and Authorization
SC - System and Communications Protection
SI - System and Information Integrity
SA - System and Services Acquisition

Control Family	**800-53 Mapping**
Contractors and Outsourced Operations / Acquisitions	SA-9, SA-11, SA-12, PM-9
Internet Availability	
Device Default Configuration	
Program Management	PM-1, PL-2, PL-3
Senior Information Security Official	PM-2
Information Security Resources	PM-3
Plan of Action and Milestones Process	PM-4, CA-5
Information System Inventory	PM-5
Information Security Measures of Performance	PM-6
Enterprise Architecture	PM-7, PL-8
Critical Infrastructure Plan	PM-8
Risk Management Strategy	PM-9
Security Authorization Process	PM-10
Business Process Definition	PM-11
Information Security Workforce	PM-13
Continuous Monitoring	PM-14, SI-4
Threat Awareness Program	PM-16, SI-5
System Boundary	
Credit Card System and Information Protection	
Privacy	PL-5

Recovery Planning	CP
Business Continuity Program (Business Environment)	CP
Disaster Recovery Program	CP
Contingency Planning	CP
Systems Development Life Cycle (SDLC)	
Configuration Management	CM
Baseline Configuration	CM-2
Change Management	CM-3
Change Classification	
Inventory (Asset Management)	CM-8, PM-5
Security Assessment and Authorization	CA-6
Security Controls Assessment	
Information Exchange Agreements	AC-20, SA-9, CA-3
Network Monitoring	SI-4, AC-2, AU-12, CA-7, CM-3, SC-5, SC-7
Vulnerability Scanning	RA-5
Internal Scanning	
External Scanning	
Ad-Hoc Scanning	
Penetration Testing	CA-8, SI-6
Data Protection (Data Security)	SI-12
Data Classification	
Data Storage (data at rest)	
Data Transmission (data in transit)	
Data Destruction	MP-6
Data Inventory	
Mobile Computing Devices	AC-19
Mobile Device Policy	
Mobile Device Configuration Requirements	
Personnel Security	PS
Monitoring of Personnel	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
Screening	**PS-3**
Access Agreement	PS-6
Transfer/Termination	**PS-5, PS-4**
Discipline	PS-8
Security Awareness Training	AT, PL-4
Physical Security	PE
Physical Access Control	**PE-2, PE-3, PE-4, PE-5**
Monitoring of Physical Environment	CA-7, PE-3, PE-6, PE-20
Emergency Procedures (power, lighting, shutoff)	**PE-10, PE-11, PE-12**
Environmental Controls (thermal, water, fire)	**PE-13, PE-14, PE-15**
Media Protection	MP-1, MP-2, MP-7

Media Marking (cover sheet, backups)	MP-3
Media Storage (confidential is locked)	MP-4
Media Transport (move from 6.1.5)	MP-5
Media Sanitization and Reuse	MP-6
incident Response (Response Planning)	IR
Incident Response Training	
Incident Categorization	CP-2, IR-4, IR-5, IR-8
Incident Handling	IR-4
Incident Reporting	IR-6
Postmortem	CA-7, RA-3, RA-5, IR-4
Maintenance	
Identification and Authentication (Identity Management)	IA
User Identification and Authentication	IA-2, IA-4, IA-5
Device Identification and Authentication	IA-3
Multi-Factor Authentication (MFA)	IA-2
Access Control	AC
Access Request	AC-3
Access Authorization (Least Privilege)	AC-6
Access Provisioning	PL-4
Network Authentication	
Separation of Duties	AC-5
Privileged User Access (Default Passwords)	IA-5
Inactive Accounts	
Failed Logon Attempts	AC-7
Password Confidentiality	
Credential Compromise	
Session Lock	AC-11
Password Reset	
UNIX/Linux System Access	
Remote Network Access	AC-17
System Use Notification	AC-8
Audit Logging	AU
Logging (Anomalies and Events)	AU
Logging Capacity	AU-4
Logging Review	AU-6
Time Stamps	AU-8
Protection of Logs	AU-9
External Provider Logs	AU-16
Systems and Network Communications Security	SC
Network Segmentation	
Denial of Service Mitigation	SC-5
Resource Availability (prioritization of resources based on criticality)	SC-6

Boundary Protection	SC-7
Session Timeout	SC-10, AC-11
Certificates	SC-17
Voice over Internet Protocol (VoIP)	SC-19
Name Address Resolution	SC-20, SC-21
Wireless Network Security	AC-18, SC-40
Restricted Ports, Protocols, and Services	CM-7
System Integrity	SI
Vulnerability Remediation	SI-2
Malicious Code Protection	SI-3, SI-8
Email Protection	SI-8
Input Checking	SI-9, SI-10
Cryptography (Encryption)	SC-12, SC-13, SC-28