

Technology Management and Deployments**1.7.2****PURPOSE**

The purpose of this policy is to ensure the City of San José's information and communications technologies support the delivery of municipal services to the community. The City prioritizes service approaches that yield resilience, security, cost-optimization, and responsiveness. This policy couples with the [Information Technology Guidelines](#) and the [Information and Systems Security Policy](#) Section 1.7.6 to form the foundation of Citywide technology management standards, protocols, and practices.

SCOPE OF APPLICATION

This policy applies to all City employees (permanent or temporary), contractors, and volunteers.

AUTHORITIES

These policies are set forth under the following authorities:

- San José City Charter Article VII, City of San José Municipal Code §2.04.3000 Information Technology Department (ITD).
- City Administrative Policy Manual Section 5.1.9, [Procurement of Information Technology](#).

RESPONSIBILITIES

The following individuals and Departments are responsible for the City's technology management standards, protocols, and practices:

- City employees are required to adhere to the processes and controls described in this policy in the performance of tasks relating to the deployment and management of information technology (IT). Failure to comply with the provisions of this policy may result in disciplinary action.
- The City's Chief Information Officer (CIO) or designee is responsible for:
 - Directing City IT resources, policies, projects, services, and coordinating across City departments.
 - Reviewing and making recommendations regarding all technology-related budget requests to the City Manager's Budget Office to ensure that investments support Citywide technology plans and strategy.
 - Coordinating with the Human Resources Department regarding all IT-related classifications and the hiring of the City's senior IT managers.
- The City Information Security Officer (CISO) is responsible for:
 - Reviewing, setting, and making recommendations on all information and systems security requirements to support Citywide technology use and resilience.
- Departments must identify their operational needs for technology personnel, goods, and services, and ensure that their technology requirements are coordinated with the IT Department and the City's Budget Office, in order to ensure proper deployment, management, and long-term maintenance.
- The Finance Department (Purchasing Division) is responsible for reviewing and carrying out all technology procurement requests as approved by the City's Chief Information Officer or designee and the Purchasing Division's prioritization process and group.

Technology Management and Deployments 1.7.2

- The City Manager's Budget Office is responsible for working with City departments to determine whether and how to fund technology operations and projects.

DEFINITIONS

- **Change Control:** The process of regulating changes to technology assets that protect uptime and availability, performance, and integrity of systems.
- **Critical and Essential Systems:** Those business and communications systems that directly impact the life/safety of the community, fiscal viability, and/or mandatory regulatory compliance of the City.
- **Executive Steering Committee:** A group of project sponsors and stakeholders responsible for making key decisions for a project.
- **Functional Lead(s):** The individual(s) responsible for communicating core business requirements and functional capabilities.
- **Independent Verification and Validation:** Review process by a third party not involved in a project's execution to confirm scope, schedule, resources, and value progress and/or delivery.
- **Technology Product:** Any on-going information technology system, software, hardware, or feature owned by the City.
- **Operations Management:** The day-to-day maintenance, performance, and monitoring of all technology products and infrastructure.
- **Product Management:** The process of planning and coordinating the value produced by a technology solution, including associated staff, features, and resources applied over the course of its lifecycle.
- **Product Owner:** The individual responsible and accountable for defining the value a technology product must deliver to meet a specific business need.
- **Products-Projects Manager:** The individual responsible for working with stakeholders to define portfolio and product roadmaps, manage execution of new products and features, and then transition changes into reliable operations.
- **Project Charter:** A planning document that lays out committed scope, timeline, value, risks, and resources of a project.
- **Project Management:** The application of processes, knowledge, and focus to deliver specific objectives within agreed parameters of time, resources, scope, and value to the organization, followed by transitioning the initiative to a maintenance state.
- **Roadmap:** Identifies the current and future needs of a product or portfolio and plans for their successful ongoing service delivery.
- **Service Owner:** The entity responsible for the ongoing operation, technical documentation, maintenance, updates/patching, and fulfillment of service levels with the product owner.
- **Sponsor:** City executive accountable for the success of an initiative, assignment of resources, resolution of project obstacles, definition of long-term value, and final decisions.
- **Technical Lead(s):** The individual(s) responsible for ensuring technology solutions, architecture, and practices deliver the required performance, features, and maintainability required by the assigned product and/or project.
- **Technology:** The computing software and hardware used to store, communicate, and analyze information, collaborate, and/or enhance work processes.

Technology Management and Deployments

1.7.2

- **Technology Interoperability:** The ability of technology systems and products to integrate and function effectively within a broader IT environment.
- **Total Cost of Ownership:** The cost of maintaining and operating a product over a default lifecycle.

POLICY

1. Controls

The Information Technology Department is responsible for ensuring that departments manage the City's information and systems assets to meet the operational, security, resilience, and resource outcomes required by the organization. This includes Citywide adherence to effective policies and protocols for planning, maintenance, change, project execution, cybersecurity, staffing, acquisition, and other processes.

Budget requests for information and communications technologies must be reviewed and approved by the requesting Department, IT Department, and the City Manager's Budget Office, to ensure that adequate resources are available to support the product over a default lifespan. The City Council makes final budget decisions, as appropriate.

ITD will evaluate technology-related procurement requests based on the product's architecture and supportability within the City environment, cost-effectiveness, project management, reliability, and security. City departments will work with the Information Technology Department to align requests to the City's technology and security standards, as well as its management policies and protocols.

Prior to procurement, resources need to be identified for all associated personnel, goods, services, and maintenance over a default product life by the requesting department.

2. Strategic and Portfolio Management

Strategic and portfolio planning, including management of support, product roadmaps, and projects, must be conducted at least annually in accordance with the [Information Technology Guidelines](#).

Portfolio Roadmaps, which guide investments, functional capabilities, system updates/upgrades, and decision-making for a portfolio, must be created for all critical and essential systems.

3. Product Management

The Product Owner and Products-Projects Manager shall:

- Jointly manage the value of City products;
- Identify criticality (life/safety/regulatory/financial); and
- Identify and engage stakeholders.

The Products-Projects Manager and the Product Owner must work with stakeholders key to the success of major technology products to create a product roadmap that shall guide investment and decision making for those assets.

Technology Management and Deployments 1.7.2

4. Operations Management

The management, maintenance and usage of all technology products must adhere to and reflect the following goals and requirements:

- Target service levels for all products;
- All products must be between one major version and 3 updates of the latest release; and
- The use and management of products must account for and mitigate cybersecurity risks.

All IT assets must be tracked and accounted for in a central asset database provided by the IT Department, along with required information. Funding requests and security allowances will not be recommended or approved for systems not identified and current in the central asset database.

All IT systems must have regularly occurring maintenance windows.

The maintenance of all technology products must follow the [Change Management Protocols](#) established by the IT Department for addressing issues and changes. These protocols factor in business continuity, technology interoperability factors, and cybersecurity value/risk of the product.

Staff required for the proper maintenance of all core and essential systems must be identified by the Service Owner and/or Product Owner.

- Staff must have clearly defined roles outlined in the product roadmap.
- Staff must be answerable to the system/product owner.
- Staff must complete all necessary training plans for effective system administration.

Performance metrics for technology products and services must adhere to service levels published by the IT Department on the City intranet. Department Product Owners and the IT Department may establish higher service levels where needed and funded, under a signed Service Level Agreement Memo. All critical and essential systems in the City must be monitored for up-time/availability and alerts set to notify of outages. Standard measures for City IT services shall be defined in the [Information Technology Guidelines](#).

5. Project Initiation and Planning

Project Initiation and Planning (Project Chartering)

- Project Charters serve to ensure that projects are thoroughly planned out in order to effectively meet goals.
- Project Charters, which must be approved by all stakeholders designated by the Sponsor(s), Product Owner, and/or Products-Projects Manager, shall be required for projects meeting Project Management Office (PMO) standards of cost, duration, complexity, and sensitivity. Refer to the City's [IT Product-Project Management Engagement Standards](#).
- Project Charters shall adhere to the City IT Product-Project Management template maintained on the Project Management Office Resource Page and the [City website](#). Project planning must account for and mitigate major risks, including cybersecurity.
- All City projects require a Sponsor, Product Owner, and Products-Projects Manager.

Project Execution

- Acquisition/Procedures

Technology Management and Deployments 1.7.2

- Projects meeting the City's IT Product-Project Management Engagement Standards will be required to follow Project Management Office Standards.
- Projects with first-year costs that exceed the [City Manager's contracting authority](#) must incorporate the Total Cost of Ownership (TCO) model, unless an exception is made by Purchasing and ITD. TCO looks at the hardware, software, maintenance and support, and professional services required for a solution over its engineered life, which is usually at least three to five years.
- Procurements must follow applicable [Guidelines](#) provided on the Finance >> Purchasing Intranet Page.
- Staffing
 - An IT Department designee(s) must be a member of the Executive Steering Committee for all critical and sensitive technology projects.
 - All projects must have at least one functional and one technical lead working together and named in the Project Charter.
 - The Project Management Office must identify products-projects management capacity during the project chartering process and provide training on City methodologies.
 - The hiring and oversight of consultant project managers must involve the City Chief Information Officer or their designee. Minimum consultant qualifications are in the [Information Technology Guidelines](#).
 - The payment of consultant project managers must be tied to delivery of milestones that adequately balance risks.
 - The IT Department has the authority to approve all department or contracted Products-Projects Managers to ensure completion of ITD training plans and meet the qualifications listed in the [Information Technology Guidelines](#).
 - Vendors will be responsible for the upkeep of technical and project documentation in order to assure that effective knowledge transfer is conducted to ensure staff effectiveness.
- Managing Testing and Load
 - Test environment usage must be well coordinated and deliver high availability and a positive customer experience. Refer to the [Information Technology Guidelines](#).
 - Products-Projects Managers must coordinate with functional and technical leads to identify and then coordinate the work of testing staff based on project requirements.

Monitoring and Controlling

- Project monitoring and reporting must be done by the Products-Projects Manager and the Project Management Office to ensure the timely and successful deployment of defined deliverables, as well as effective scope and change control.
- The IT Department has the authority to cancel or hold all approved projects, and shall be required to evaluate and remediate any project in which any of mitigation events listed in the [Information Technology Guidelines](#) occur.
- Status reports, as defined in the [Information Technology Guidelines](#), must be published by the Project Management Office to stakeholders and the Executive Steering Committee on at least a quarterly basis for all projects designated by the Project Management Office.
- Upon completion of the project charter, a project status dashboard must be provided by the Project Management Office on at least a quarterly basis and populated with relevant project status information. The IT Department may designate a more or less frequent reporting cadence based on the impact and criticality of a specific project. Future work on un-reported projects shall be suspended until status is verified by the City Chief Information Officer or their designee.
- Independent Verification and Validation (IV&V) will be conducted by the Project Management Office for critical and high-risk projects in accordance with the Information

Technology Management and Deployments

1.7.2

Technology Guidelines. An independent contractor will conduct IV&V for projects considered High Priority as described in the [Information Technology Guidelines](#) when deemed appropriate and necessary.

- Project Charters and amendments, key communications and approvals, and status reports must be documented by the Products-Projects Manager and project staff through the Project Management Office designated repository, and must be accessible to all assigned City staff and vendor staff.

Project Closure

- Project closure practices should ensure the orderly conclusion of a project and transition to operations.
- The Executive Steering Committee, as established during the project chartering process, must sign-off on the project charter to close the project once pre-requisites in the [Information Technology Guidelines](#) are met.
- Products-Projects Managers must complete a lessons-learned session with project team members at the conclusion of a project.



6. Security Practices and Controls

All staff and contractors involved in the deployment and management of information technology must comply with the provisions of the [Information and Systems Security Policy](#), City Administrative Policy Manual Section 1.7.6, as well as the [Procurement of Information Technology Policy](#), City Administrative Policy Manual Section 5.1.9.

All critical and essential City Information Systems must have an Information System Contingency Plan (ISCP), as defined by the National Institute of Standards and Technology (NIST).

Approved on October 11, 2015, SB 272 adds a section to the California Public Records Act requiring local agencies to create a catalog of Enterprise Systems and update that catalog at least

